Alarm Control Panel

VERSA

Firmware Version 1.10

PROGRAMMING

versa_p_en 09/21

SATEL sp. z o.o.
ul. Budowlanych 66 • 80-298 Gdańsk • POLAND
tel. +48 58 320 94 00
www.satel.eu

Before you start programming, please read carefully this manual in order to avoid mistakes that can lead to malfunction or even damage to the equipment.

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software. Current information about the changes being introduced is available on our website.
Please visit us:
https://support.satel.eu

The declaration of conformity may be consulted at www.satel.eu/ce

Service code: 12345

The following symbols may be used in this manual:

- note,
- caution.

Changes made to the firmware versions 1.08 and 1.09

Global parameters	New option: BACKLIGHT OFF ON AC LOSS.
Partitions	New option: ENTRY DELAY IN NIGHT ARM.
Ethernet module	Changed names of options: – SATEL SERVER (LAN) has been replaced with LAN, – GET DATE AND TIME FROM A TIME SERVER (LAN) has been replaced with LAN. New options: – DO NOT REPORT SATEL SERVER CONNECTION TROUBLE, – ALARM 3 INCORRECT CODES (MOBILE APPLICATION).
ABAX wireless system	If the ACU-120 / ACU-270 controller with firmware version 5.03 is connected to the control panel: – you can select whether the AMD-101 detector is to occupy one or two positions on the list of wireless devices, – the users can replace batteries in the wireless keypad after starting the REPLACE BAT. function. APT-100 keyfob LEDs can indicate that partitions are disarmed.
E-mail messaging	Changed name of option: E-MAIL MESSAGING (LAN) has been replaced with LAN.
Entering code	After an incorrect code has been entered, the “Wrong code” message will be displayed on the LCD keypad. The same message will also be displayed after entering a correct code, when the keypad is blocked.
User functions	A new function in the 0.SERVICE submenu: 9.REPLACE BAT.

CONTENTS

1. Introduction

The VERSA alarm system can be configured by using:

- keypad,
- computer with DLOADX program installed (locally or remotely).

Local programming (using the keypad or DLOADX program) is possible, if one the following conditions is met:

- PERMANENT ACCESS option is enabled (SERV. ACCESS user function ([code] [*] ▶0. SERVICE ▶5. SERV. ACCESS) – see: USER MANUAL) – the option is enabled by default,
- access to the control panel has been granted temporarily to the service personnel (ACCESS TIME user function ([code] [*] ▶0. SERVICE ▶6. ACCESS TIME) – see: USER MANUAL).

As required by the standards, the service access after completion of the installation has to be limited by the administrators.

2. Configuring the control panel with keypad

The control panel can be programmed using the functions available in the service mode. In case of the LED keypad, programming is subject to some limitations (e.g. entering names is impossible). **Programming the control panel by use of LED keypad is not recommended by SATEL.**

The service mode is indicated on the keypads by means of the LED. The LED is lit on the keypad in which the service function menu is available, while it is blinking on all the other keypads. The service mode may also be signaled acoustically, after the corresponding option is enabled. Additional information is provided by the LED, which is:

– blinking during navigation throughout the menu and submenus,
– lit when any service function is running.

When in the service mode, the alarm system signals no alarms.

2.1 Starting the service mode

1. Enter the **service code** (by default: 12345) and press the [*] key.
2. Press in turn [0] [0] [#]. The service mode will be started.

2.2 Starting the service mode “from pins”

When entering the service mode in the normal way is not possible (the control panel does not support keypads, does not accept the service code, etc.), you can use the emergency procedure, so-called, starting “from pins”.

1. Power off the control panel (disconnect AC mains first, and the battery next).
2. Place a jumper across the RESET pins.
3. Power up the control panel (first connect the battery and then the AC power).
4. Wait a few seconds and remove the jumper from the RESET pins. The control panel will enter the service mode. The service mode menu will be available on the keypad with the lowest address (in the case of the wireless keypad, the menu will be displayed after pressing any key).

If the SERVICE MODE FROM RESET PINS option is disabled in the control panel then, depending on the type of keypad in which the lowest address is set:

- *LCD: the , and LEDs of the second partition will be lit, and the message "Restore factory settings ? 1=Yes" will come up on the display,*
- *LED: the and LEDs of the second partition will be lit and the LED will be blinking rapidly.*

Pressing the [1] key will restore the factory default settings of the control panel, thus making it possible to enter the service mode.

2.3 Navigating through the menu and running functions

2.3.1 Using the arrow keys

This method is only available in the LCD keypad.

1. Using the [▼] and [▲] keys, find the required submenu (the submenu indicating cursor: ›).
2. Press the [▶] or [#] key to enter the submenu (use the [◀] key to return to the previous menu/submenu, and the [*] key to return to the main menu).
3. Repeat the steps 1 and 2 until the required function is found (the function indicating cursor: ÷). Press [▶] or [#] to start the function.

2.3.2 Using the digit shortcuts

Submenus and functions are numbered. In order to enter a submenu, just press the key with number corresponding to the submenu number. In order to start a function, press the key with number corresponding to the function number, and then [#]. You can quickly start the selected function by entering at once a sequence of some digits (corresponding to the consecutive submenu numbers and the function number) and pressing [#].

For example, to start the expander identification function, press in turn the [2abc] [1] [1] [#] keys, where:

[2abc] - entering the 2. HARDWARE submenu,

[1] - entering the 1. KPDS. & EXPS. submenu,

[1] [#] - running the 1. IDENTIFICAT. function.

In the LCD keypad, use the [*] key to return from a submenu to the main menu or from a function to a submenu, and use the [◀] key to return from a submenu to the previous menu/submenu.

In the LED keypad, use the [*] key to return to the main menu.

Remember that the sequence of digits which starts a function e.g. from the main menu level will not start the same function from the submenu level.

2.4 "Step by step" programming method

In case of some functions (e.g. configuring the zones, outputs, expanders, etc.), the programming is effected by using the "step by step" method. After calling the function and selecting the item to be configured from the list, the first parameter available for programming will be displayed. After pressing [#], you will go on to programming another parameter (if you have entered some changes, they will be saved). Having programmed all parameters, you will return to the submenu (LCD keypad) / main menu (LED keypad). The and

LEDs of the first and second partition show the number of programming step (see: page 10 table 4). Some programming steps may be sometimes not available.

2.5 Entering data

The changes entered will be saved after pressing the # key. Use the * key to quit the function without saving changes.

2.5.1 LCD keypad

The data being entered are presented on the display. The method of programming depends on the type of data to be entered by service function.

Selection from the single-choice list

In the upper line of the display, the function name is presented, and in the lower one – the currently selected item. You can scroll through the list using the ▼ and ▲ keys. The ▶ and ◀ keys are not used.

Selection from the multiple-choice list

In the upper line of the display, the function name is presented, and in the lower one – one of the items to choose from. You can scroll through the list using the ▼ and ▲ keys. The following symbol is situated in the upper right corner of the display:

■ – displayed item is selected / option is enabled,

· – displayed item is not selected / option is disabled.

Press any numerical key to change the currently shown symbol for another one.

If you want to see the status of all items (these can be e.g. zones, outputs, options, etc.), press ▶ or ◀. The numbers around the display allow the items to be identified. Use the ▶ and ◀ keys to move the cursor. After hovering the cursor over the selected item, you can change its status by pressing any numeric key. If you want to restore the previous way of presentation of the list, press ▼ or ▲.

Entering decimal values

To enter digits, use the numeric keys. The ▶ key moves the cursor to the right, and the ◀ or ▲ key – to the left.

Entering hexadecimal values

To enter digits, use the numeric keys, and to enter characters from A to F, use the 2abc and 3def keys (keep pressing the key until the required character appears). The ▶ key moves the cursor to the right, and the ◀ or ▲ key – to the left.

Programming telephone numbers

To enter digits, use the numeric keys, and to enter other characters, use the 1, 2abc, 3def and 0 keys (keep pressing the key until the required character appears – see: table 1). You can enter up to 16 characters. Some of the characters occupy two positions (a, b, c, d, # and ✣). If they are used, you can enter less characters than 16.

Shown on the right side in the upper line of the display is information about the letter case: [ABC] or [abc] (it will be displayed after pressing any key and will be visible for a few seconds after the last keystroke). Use the ▶ and ◀ keys to move the cursor. The ▲ key deletes the character on the left side of the cursor.

Characters available after next keystroke										
key	mode [ABC]					key	mode [abc]			
1	1	#				1	1	#		
2abc	2	B	C			2abc	2	a	b	c
3def	3	D	E	F		3def	3	d		
4ghi	4					4ghi	4			
5jkl	5					5jkl	5			
6mno	6					6mno	6			
7pqrs	7					7pqrs	7			
8tuv	8					8tuv	8			
9wxyz	9					9wxyz	9			
0	0	*				0	0	*		

Table 1. Characters available in the keypad when entering telephone numbers (to change the letter case, press).

Special character	Function description
B	switch-over to pulse dialing
C	switch-over to tone dialing (DTMF)
D	waiting for additional signal
E	3 second pause
F	10 second pause
*	signal * in DTMF mode
#	signal # in DTMF mode
a b c d	other signals generated in DTMF mode

Table 2. Special character functions.

Entering names

The characters that can be entered by using the keys are presented in Table 3. Keep pressing the key until the required character appears. Long press the key to display the digit assigned to it.

Shown on the right side in the upper line of the display is information about the letter case: [ABC] or [abc] (it will be displayed after pressing any key and will be visible for a few seconds after the last keystroke).

The key moves the cursor to the right, and the key – to the left. The key deletes the character on the left side of the cursor.

Key	Characters available after next keystroke																	
1	!	?	'	`	↵	"	{	}	$	%	&	@	\	^	|		#	1
2abc	a	b	c	2														
3def	d	e	f	3														
4ghi	g	h	i	4														
5jkl	j	k	l	5														
6mno	m	n	o	6														
7pqrs	p	q	r	s	7													
8tuv	t	u	v	·								8						
9wxyz	w	x	y	z	9													
0		.	,	:	;	+	-	*	/	=	_	<	>	(	)	[	]	0

Table 3. Characters available when entering names. The upper case letters are available under the same keys (to change the letter case, press).

2.5.2 LED keypad

The data being entered are presented by means of LEDs. The method of programming depends on the type of data to be entered by service function.

Selection from the single-choice list

The lit LEDs show the available items on the list. Blinking LED indicates the current position of the cursor and, consequently, the item which is currently selected. Use the and keys to move the cursor. The and keys are not used.

Selection from the multiple-choice list

The status of all items available within the function (including e.g. zones, outputs, options, etc.) is illustrated by LEDs designated by numbers. The steady-on LEDs indicate the selected items. The blinking LED indicates that that the cursor is there. Use the and keys to move the cursor. Press any numeric key to change the LED status (to turn it ON or OFF). The and keys are not used.

Entering decimal values

To enter digits, use the numeric keys. Up to 6 digits can be presented on the LEDs. Each digit is presented on four LEDs – see Table 4. LEDs 1-4 present the first digit, LEDs 5-8 – the second, LEDs 9-12 – the third, LEDs 16-19 – the fourth, LEDs 20-23 – the fifth, and LEDs 24-27 – the sixth digit. The arrow keys are not used. The value entered can only be corrected after restarting the function.

Entering hexadecimal values

To enter digits, use the numeric keys, and to enter characters from A to F, use the 2abc and 3def keys (keep pressing the key until the required character appears). Up to 6 characters can be presented on the LEDs. Each character is presented on four LEDs – see Table 4. LEDs 1-4 present the first character, LEDs 5-8 – the second, LEDs 9-12 – the third, LEDs 16-19 – the fourth, LEDs 20-23 – the fifth, and LEDs 24-27 – the sixth character. The arrow keys are not used. The value entered can only be corrected after restarting the function.

LED status	Digits and characters
☐ ☐ ☐ ☐	0
☐ ☐ ☐ ■	1
☐ ☐ ■ ☐	2
☐ ☐ ■ ■	3
☐ ■ ☐ ☐	4
☐ ■ ☐ ■	5
☐ ■ ■ ☐	6
☐ ■ ■ ■	7
■ ☐ ☐ ☐	8
■ ☐ ☐ ■	9
■ ☐ ■ ☐	A
■ ☐ ■ ■	B
■ ■ ☐ ☐	C
■ ■ ☐ ■	D
■ ■ ■ ☐	E
■ ■ ■ ■	F

☐ – LED OFF

■ – LED ON

Table 4. The binary mode of presenting digits and characters.

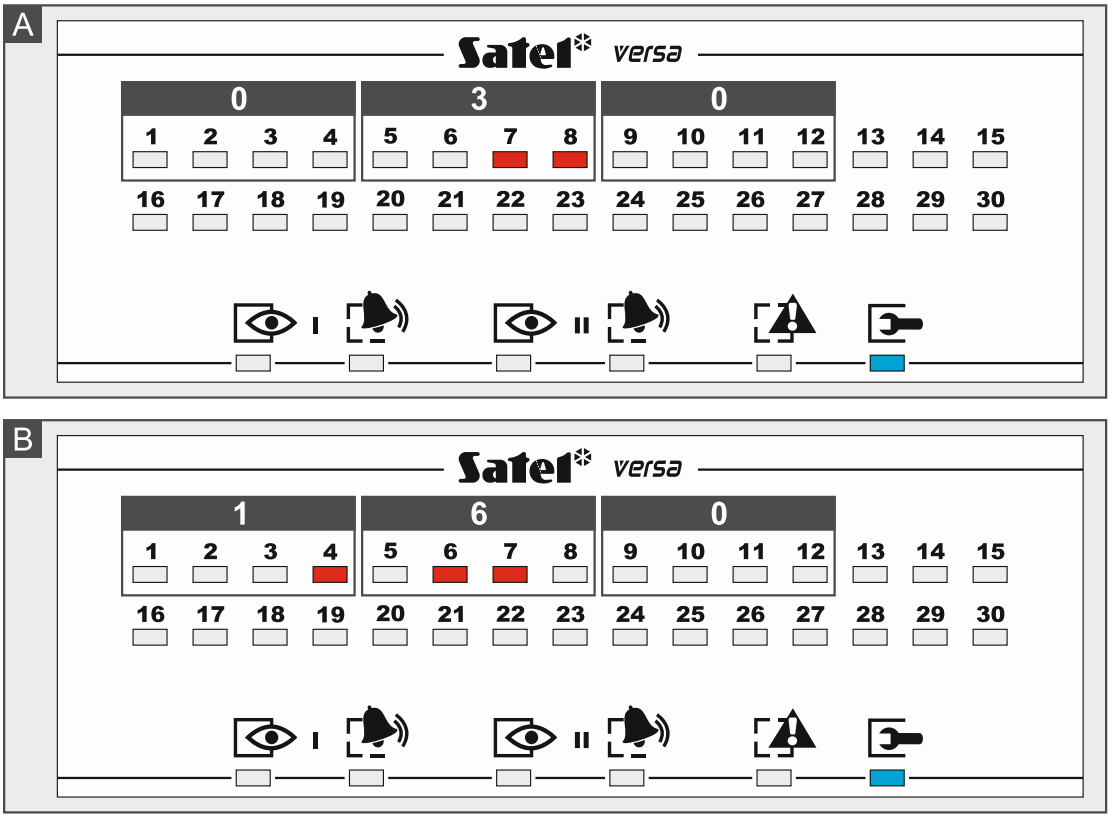


Fig. 1. Examples of presenting decimal values by means of LEDs in the LED keypad. Value 30 (030) is programmed in Example A, and value 160 in Example B.

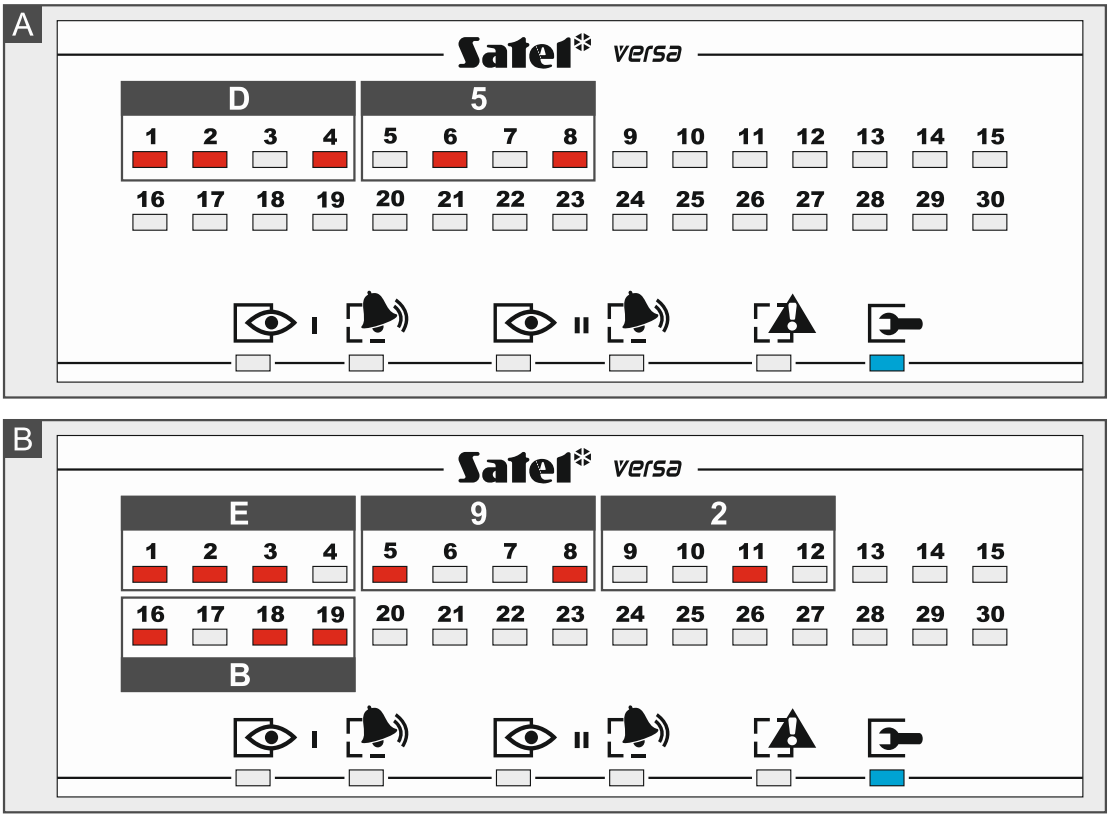


Fig. 2. Examples of presenting hexadecimal values by means of LEDs in the LED keypad. Two-character value D5 is programmed in Example A, and four-character value E92B in Example B.

Programming telephone numbers

The telephone numbers are entered in much the same way as in the LCD keypad, however the LEDs can only present the first 6 characters (only digits and characters B, C, D, E and F – see: Table 4). The arrow keys are not used. The value entered can only be corrected after restarting the function.

2.6 Service mode menu

Shown in square brackets are sequences which enable calling up a particular submenu or starting a particular function from the main menu level.

0. SrvMod config

- [00#] 0. Serv.Mode end
- [01#] 1. VERSA id.
- [02#] 2. DLOADX id.
- [04#] 4. DLOADX tel.
- [06#] 6. SrvMod opt.
- [07#] 7. Restore all
- [08#] 8. Default usr.
- A. Hide SM now

1. Partitions

- [11#] 1. Part. 1 zones
- [12#] 2. Part. 2 zones

- [13] 3. Part. 1 times
  - [131#] 1. Exit delay
  - [132#] 2. Entry delay
  - [133#] 3. Warning
  - [134#] 4. Verification
  - [135#] 5. Autoarm delay
  - [136#] 6. A-arm defer
- [14] 4. Part. 2 times
  - [141#] 1. Exit delay
  - [142#] 2. Entry delay
  - [143#] 3. Warning
  - [144#] 4. Verification
  - [145#] 5. Autoarm delay
  - [146#] 6. A-arm defer
- [15#] 5. Part. 1 name
- [16#] 6. Part. 2 name
- [17#] 7. Part. options

2. Hardware

- [21] 1. Kpds. & exps.
  - [211#] 1. Identificat.
  - [212#] 2. Settings
    - [select device]
  - [213#] 3. Wireless dev.
    - [213#1#] 1. New device.
    - [213#2#] 2. Config. device
    - [213#3#] 3. Remove device
    - [213#4#] 4. Wirelss.zones
    - [213#5#] 5. Synchronize
    - [213#6#] 6. Test mode on
    - [213#7#] 7. Test mode off
    - [213#8#] 8. Connect msg.
  - [214#] 4. Options
  - [217#] 7. Rem.ABAX dev.
  - [218#] 8. Rem.ABAX kfbs
  - [219#] 9. Rem.RX k-fobs
  - [210#] 0. Keypads addr.
- [22#] 2. Zones
  - [select zone]
- [23#] 3. Outputs
  - [select output]
- [24] 4. Quick control
  - [241#] 1. Control 1#/1*
  - [242#] 2. Control 2#/2*
  - [243#] 3. Control 3#/3*

- [244#] 4. Control 4#/4*
- [245#] 5. Control 5#/5*
- [246#] 6. Control 6#/6*
- [247#] 7. Control 7#/7*
- [248#] 8. Control 8#/8*
- [249#] 9. Control 9#/9*
- [240#] 0. Control 0#/0*

- [25#] 5. EOL 1 resist.
- [26#] 6. EOL 2 resist.
- [27#] 7. VERSA zones

3. Global param.

- [31#] 1. Options
- [32#] 2. Kpds al. time
- [33#] 3. Hide arm st.
- [34#] 4. AC trbl. delay
- [35#] 5. Tel. trbl. del.
- [36#] 6. RTC adjustm.
- [37#] 7. Daylight sav.
- [38#] 8. Summer time
- [39#] 9. Winter time
- [30#] 0. Min.code len.

4. Timers

- [41#] 1. Timer 1 name
- [42#] 2. Timer 2 name
- [43#] 3. Timer 3 name
- [44#] 4. Timer 4 name

5. Monitoring

- [50#] 0. Stations
- [51] 1. Station 1
  - [511#] 1. Tel. number
  - [512#] 2. Tel. format
  - [513#] 3. Options
  - [514#] 4. Attempts no.
  - [515#] 5. Suspens. time
  - [516] 6. Identifiers
    - [5161#] 1. Id. 1
    - [5162#] 2. Id. 2
    - [5163#] 3. Id. 3
    - [5160#] 0. System Id.
  - [517#] 7. T-M/SIA pref.
  - [518#] 8. StationTCP/IP
  - [519#] 9. SIA-IP acct
- [52] 2. Station 2
  - [521#] 1. Tel. number

- [522#] 2. Tel. format
- [523#] 3. Options
- [524#] 4. Attempts no.
- [525#] 5. Suspens. time
- [526] 6. Identifiers
  - [5261#] 1. Id. 1
  - [5262#] 2. Id. 2
  - [5263#] 3. Id. 3
  - [5260#] 0. System Id.
- [527#] 7. T-M/SIA pref.
- [528#] 8. StationTCP/IP
- [529#] 9. SIA-IP acct

[53#] 3. SIA options

[54] 4. Event codes

- [541] 1. Partition 1
  - [5411#] 1. Arm by user
  - [5412#] 2. Arm other
  - [5413#] 3. Quick arm
  - [5414#] 4. Disarm by usr
  - [5415#] 5. Disarm other
  - [5416#] 6. Rest. by user
  - [5417#] 7. Restore other
  - [5418#] 8. Duress
  - [5419#] 9. Arming failed
- [542] 2. Partition 2
  - [5421#] 1. Arm by user
  - [5422#] 2. Arm other
  - [5423#] 3. Quick arm
  - [5424#] 4. Disarm by usr
  - [5425#] 5. Disarm other
  - [5426#] 6. Rest. by user
  - [5427#] 7. Restore other
  - [5428#] 8. Duress
  - [5429#] 9. Arming failed
- [543] 3. Zones
  - [5431#] 1. Alarm
  - [5432#] 2. Alarm restore
  - [5433#] 3. Tamper
  - [5434#] 4. Tmp restore
  - [5435#] 5. Trouble
  - [5436#] 6. Trouble rest.
  - [5437#] 7. Bypass
  - [5438#] 8. Unbypass
- [544] 4. Wirelss.zones

[5441#] 1. Commun. loss
[5442#] 2. Commun. rst.
[5443#] 3. Battery low
[5444#] 4. Battery rst.
[545] 5. Exp. modules
[5451#] 1. Tamper
[5452#] 2. Tmp restore
[5453#] 3. Fire alarm
[5454#] 4. Medical alarm
[5455#] 5. Panic alarm
[5456#] 6. 3 wrong codes
[5457#] 7. 3 wrong cards
[546] 6. Exp. supply
[5461#] 1. AC trouble
[5462#] 2. AC restore
[5463#] 3. Batt. trouble
[5464#] 4. Batt. restore
[5465#] 5. Overload
[5466#] 6. Overload rst.
[547] 7. System
[5471#] 1. Troubles
[5472#] 2. Troubles rst.
[5473#] 3. Other
[5474#] 4. RTC setting
[540#] 0. TELIM codes
[55#] 5. Test at
[56#] 6. Test every
[57#] 7. Test (armed)

6. Messaging
[61#] 1. Zone alarms
[62#] 2. Output trig.
[63] 3. Arming
[631#] 1. Part. 1 user
[632#] 2. Part. 1 other
[633#] 3. Part. 2 user
[634#] 4. Part. 2 other
[635#] 5. Arm.p1 failed
[636#] 6. Arm.p2 failed
[64] 4. Disarming
[641#] 1. Part. 1 user
[642#] 2. Part. 1 other
[643#] 3. Part. 2 user
[644#] 4. Part. 2 other
[65] 5. Other

[651#] 1. Tamper alarm
[652#] 2. Tamper rest.
[653#] 3. AC trouble
[654#] 4. AC restore
[655#] 5. Battery trbl.
[656#] 6. Battery rest.
[657#] 7. Tel. lin. rest.

[66] 6. Message type
[661#] 1. Tel1 msg. type
[662#] 2. Tel2 msg. type
[663#] 3. Tel3 msg. type
[664#] 4. Tel4 msg. type
[665#] 1. Tel5 msg. type
[666#] 2. Tel6 msg. type
[667#] 3. Tel7 msg. type
[668#] 4. Tel8 msg. type

[67] 7. PAGER param.
[671#] 1. PAGER1
[672#] 2. PAGER2

[68#] 8. Queues/tries
[69#] 9. Messages
[60#] 0. Tel. names

7. Answering
[71#] 1. Rings to ans.

8. Usr templates
[81#] 1. Settings
[82#] 2. Key fob func.
[83#] 3. Confirmations
[84#] 4. Name

9. User menu

The 9. USER MENU function enables access to the user functions when the control panel remains in the service mode (press the * key to return to the main menu of the service mode). The user menu and functions are described in the User Manual.

2.7 Hiding the service mode

In the case of keypads with display screen, you can hide the service mode by using the HIDE SM NOW function (▶0. SRVMOD CONFIG ▶A. HIDE SM NOW). The control panel will remain in the service mode, but the service mode menu will not be displayed. The function can be useful e.g. when you have to leave the keypad, but you want to prevent unauthorized personnel from getting access to the service menu in the meantime. To get access to the menu again, proceed in the same way as when entering the service mode.

2.8 Exiting the service mode

In order to exit the service mode, use the SERV.MODE END function.

To exit the service mode, do the following:

LCD keypad: keep pressing [*] until you return to the main menu, and then press in turn [0] [0] [#],

LED keypad: press [*] and then press in turn [0] [0] [#].

3. Configuring the control panel with DLOADX program

Required program version: 1.19.004 (or newer).

Access to the program is protected by a code. The factory default code: 1234 (you need not enter the factory code, just click on the “OK” button).

The factory code should be changed.

Entering an incorrect code three times will terminate the program.

Communication between the program and the control panel is coded. The alarm control panel may be programmed locally or remotely.

3.1 Main menu of the DLOADX program

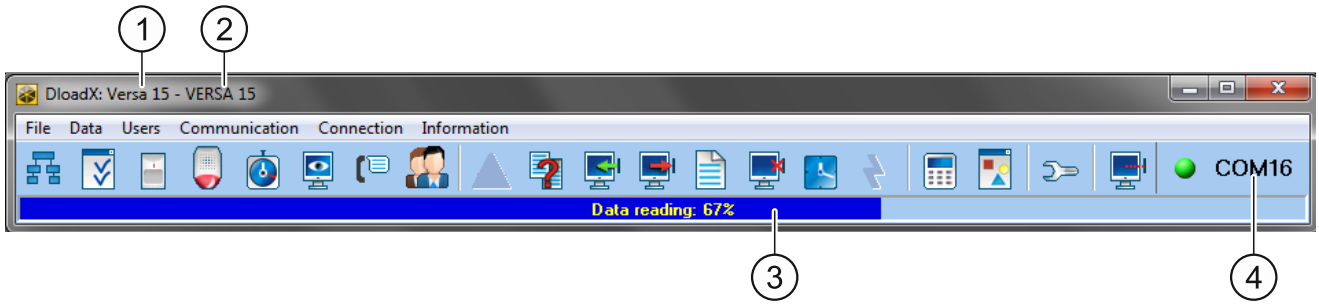


Fig. 3. Main menu of DLOADX program.

(1) type of alarm control panel.

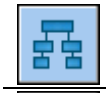
(2) name of alarm system / data file.

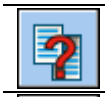
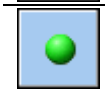
(3) information on data writing/reading progress.

(4) information on the way of communication with the alarm control panel:

COMn [n – number of computer COM port] – local connection via the RS-232 (TTL) port,
Modem – remote connection via the modem,
TCP/IP – remote connection via the Ethernet.

3.1.1 Buttons

	click to open the “VERSA – Structure” window.
	click to open the “Global parameters” window.
	click to open the “VERSA – Zones” window.
	click to open the “VERSA – Outputs” window.

	click to open the “VERSA – Timers” window.
	click to open the “VERSA – Reporting” window.
	click to open the “VERSA – Tel. messaging” window.
	click to open the “VERSA – Users” window.
	click to open the window with information on errors made when configuring the alarm system (e.g. nonconformity with requirements of EN 50131 for Grade 2, when GRADE 2 option is enabled).
	click to open the “Data comparison” window.
	click to read data from the control panel.
	click to write data to the control panel.
	click to open the event log window.
	click to terminate data reading/writing.
	click to write computer clock time to the control panel.
	click to display virtual keypad.
	click to display the drop-down menu shown in Fig. 4.
	click to open the “Configuration” window. The “Configuration” window will not open if the remote connection is established. Instead, a window with the connection information will open. Opening the “Configuration” window will only be possible after the connection is ended.
	click to display the drop-down menu, where you can select the way of communication with the alarm control panel.
	click to: – enable/disable the COM port, – open the connection information window (remote programming). Color of the button icon has the following meanings: green – connection OK, alternating green and yellow – data transfer going on, gray – no connection.

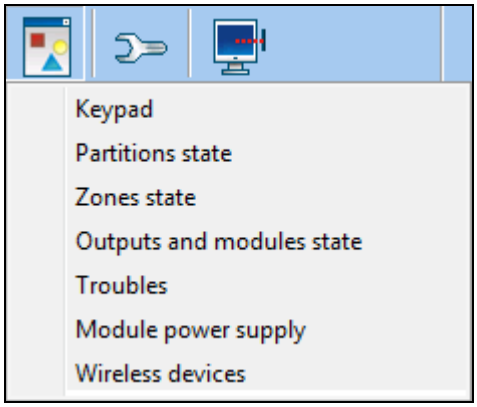


Fig. 4. Menu displayed after pressing the  button.

3.1.2 Changing the DLOADX program access code

1. Click on “File” →“Access setup” →“Change access code” (Fig. 5). Dialog window with a field for entering the code will be displayed.

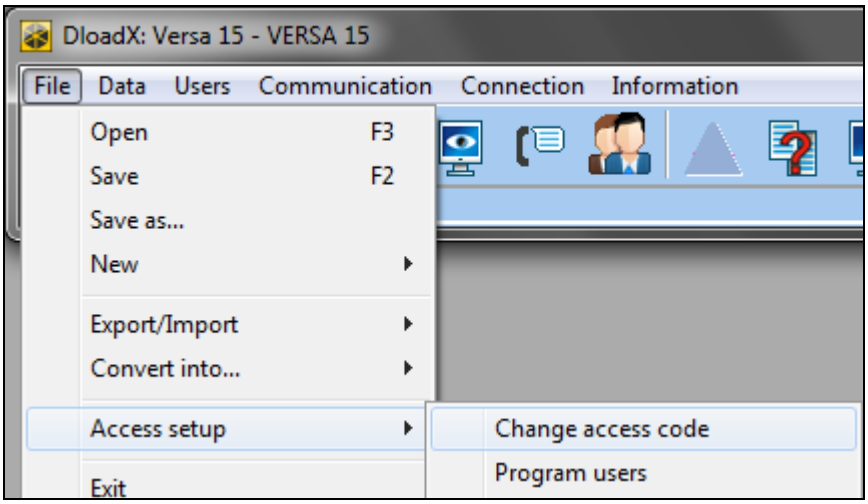


Fig. 5. Starting the procedure of changing the DLOADX program access code.

2. Enter the old access code to the program and click “OK”. Another dialog window with a field for entering the code will be displayed.
3. Enter the new access code to the program and click “OK”. Another dialog window with a field for entering the code will be displayed.
4. Re-enter the new access code to the program and click “OK”. A dialog window will be displayed with a message that the code has been changed.
5. Click “OK” to close the window and finish the procedure.

You can enter additional program access codes and define the rights of users using those access codes (“File” →“Access setup” →“Program users” – see: Fig. 5).

3.2 Parameters related to communication between the control panel and DLOADX program

3.2.1 Communication identifiers

Communication identifiers are necessary for all methods of communication.

Programming the communication identifiers

You can program the communication identifiers:

- DLOADX program: “Connection settings” window (the command for opening this window is available in the “Communication” menu; you can also use the Ctrl+R key combination).
- keypad: functions available in the SRVMOD CONFIG submenu (SERVICE MODE ▶0. SRVMOD CONFIG).

You can skip programming the communication identifiers in DLOADX program in the following cases:

- the control panel identifiers have their factory default value – after establishing connection, a prompt will be displayed asking you to write randomly generated identifiers to the control panel and the program (you can accept them or enter your own ones),
- communication is effected through the control panel RS-232 (TTL) port and the control panel is running in the service mode – after establishing connection, the DLOADX program will read the identifiers programmed in the control panel.

Description of communication identifiers

VERSA identifier – identifier of the alarm control panel. It consists of 8 characters (digits or letters from A to F). It enables the DLOADX program to recognize the control panel and match the data file to it, provided the data file has been written to the computer. Do not program the same identifier for different control panels which are operated from the same computer (the DLOADX program will be incapable of distinguishing between them).

DLOADX identifier – identifier of the computer with DLOADX program. It consists of 8 characters (digits or letters from A to F). It enables the control panel to recognize the computer with DLOADX program.

Communication between the DLOADX program and the control panel is possible, if identical identifiers are programmed in the program and the control panel.

3.2.2 Modem communication parameters

Programming the parameters

Telephone numbers

You can program the telephone numbers:

- DLOADX program: “Connection settings” window (the command for opening this window is available in the “Communication” menu; you can also use the Ctrl+R key combination).
- keypad: functions available in the SRVMOD CONFIG submenu (SERVICE MODE ▶0. SRVMOD CONFIG).

DLOADX program settings

You can configure the modem communication settings in the “Configuration” window, “Modem” tab.

Control panel settings

You can configure the modem communication settings:

- when programming the global parameters (see: “Global parameters” p. 26).

Description of parameters

Telephone numbers

Descriptions displayed on the LCD keypad are shown in square brackets.

Panel’s tel. no – telephone number of the control panel.

PC phone number [DLOADX tel.] – telephone number of the modem connected to computer with DLOADX program installed.

DLOADX program settings

After clicking on the  button you can configure the parameters of the modem connected to computer (see: “Configuring the modem connected to computer”).

Dialing – the method of dialing numbers by the modem connected to computer (tone or pulse).

Dial tones control – if option is enabled, the modem connected to computer will detect the dial tone or busy signal before dialing the number.

Speaker – operating mode of the modem speaker. The speaker can be always OFF, or ON until connection with the control panel is established (auto), or always ON.

Volume – volume of modem speaker.

Answering – how the DLOADX program reacts when the control panel is connecting to the program. Communication can be established automatically after a preset number of rings, or the program will only indicate an attempt to establish communication by the control panel (communication will only be established after clicking on the “Answer” button).

Double call – you can define duration of the pause between the first and the second call, if the control panel is set to go off-hook after the second call.

Configuring the modem connected to computer

You can edit the parameters after clicking on the “Change” button.

Port RS-232 – computer COM port to which the modem is connected.

Modem – list of modems, the parameters of which are defined. The list of modems and their settings will be written to disk in the “modem.ini” file.

Baud Rate – transmission rate of the serial port. It is recommended that the highest rate acceptable by the modem be set (only some modems may require the 300 bps setting in order to enforce operation with exactly this speed).

Reset command – the command to reset the modem. Typically, it is the **ATZ** command (reset with restoration of the user's zero profile). Some modems may require using the **AT&F** command (reset with restoration of the factory default settings).

Initializing – lines containing the modem initialization commands. In the first line: **E0V1Q0** – a command required for proper operation of the modem. You should also add the operating mode selection: **B0** or **B1** (selection of transmission format: V.21 or Bell103), and the commands limiting transmission rate over telephone line to 300 bps. These are commands specific for the given modem model, e.g. **N0S37=3**, **F1** or **+MS=1,0,300,300** etc. Information on how to limit the modem transmission rate is usually included in the device manual. The other line should contain the following commands: **S0=0S9=1S7=120S10=255**.

Control panel settings

Parameters and options related to modem communication are described in section “Global parameters” (p. 26).

3.2.3 Ethernet communication parameters

Programming the parameters

DLOADX program settings

You can configure the Ethernet communication settings in the “Connection settings” window.

Ethernet module settings

You can configure the Ethernet communication settings when programming the Ethernet module (see: “Ethernet module” p. 51).

Description of the parameters

DLOADX program settings

Connection – you can define two sets of parameters:

LAN/WAN – parameters for communication via local or wide network.

LAN: ETHM-1 – parameters for communication via local network only. In this case, the port number and data encryption key programmed in the settings of Ethernet module.

Server – address of the Ethernet module. If the Ethernet module is not in the same local network as the computer with DLOADX program, it must be a public address. You can enter either the IP address or the domain name.

Port – the number of TCP port used for communication between the control panel and computer with DLOADX program via Ethernet. You can enter a value from 1 to 65535. Default value: 7090.

DLOADX key – a string of up to 12 alphanumeric characters (digits, letters and special characters), used for data encryption during communication between the control panel and the computer with DLOADX program via Ethernet.

ETHM-1 ID – individual identification number of the Ethernet module for the purpose of communication via the SATEL server.

ETHM-1 MAC – hardware address of Ethernet module.

Control panel settings

For parameters and options related to communication via Ethernet, see section “Ethernet module” (p. 51).

3.3 Local programming

3.3.1 Starting local programming

1. Connect the control panel RS-232 (TTL) port with the computer port (for example, by means of the USB-RS converter offered by SATEL).
2. Start the DLOADX program.
3. If the control panel is connected to other computer port than COM1, click on  in the main menu. The “Configuration” window will open, in which you can select the COM port to which the control panel is connected.
4. Establish communication between the control panel and the program in one of the following ways.

Establishing communication with verification of identifiers

Use the keypad to start the local programming function [START DWNLRS]:

1. Enter the service code and press [*].
2. Press in turn [0] [3def] [#].

Establishing communication without verification of identifiers

If no communication identifiers have been programmed in the DLOADX program, use the keypad to enter the service mode:

1. Enter the service code and press [*].
2. Press in turn [0] [0] [#]. The service mode will be started and, additionally, the local programming function will be started [START DWNLRS].

Emergency communication establishing procedure ("from pins")

If the control panel does not support keypads, does not accept the service code, etc., start the service mode "from pins" (see: "Starting the service mode "from pins"" p. 5). The local programming function [START DWNLRS] will be started automatically.

3.3.2 Finishing local programming

You can finish the local programming function from the keypad by using the FINISHDWNLRS function (enter the service code and press [*], and then press in turn [0] [4ghi] [#]).

The local programming function will be finished automatically 4 hours after communication with the DLOADX program is ended.

3.4 Remote programming

3.4.1 Programming via modem

Modem communication can be established in one of the following ways:

1. Connection initialized from the DLOADX program. The control panel can be programmed from any location.
2. Connection initialized from the DLOADX program, but the control panel calls back and sets up the connection. The control panel can only be programmed from a defined location.
3. Connection initialized by the control panel. The control panel can only be programmed from a defined location. This method should be used when the system user does not want the remote programming to take place without his knowledge.

Initiating a modem connection from DLOADX program

Control panel settings:

- **do not program the telephone number of modem connected to computer!**
- enable ANSWERING – MODEM option (see: "Global options" p. 27),
- define the number of rings after which the control panel will answer incoming calls – RINGS BEFORE ANSWER (see: "Other global parameters" p. 31),
- enable the DOUBLE CALL option if the control panel is to answer only after the second call (see: "Global options" p. 27).

DLOADX program settings:

- program the telephone number of control panel,
- configure the modem communication parameters.

1. Click on the  button in DLOADX program main menu. A drop down menu will be displayed.
2. Click “Modem 300bps”. Window with modem initialization information will be displayed.
3. After modem initialization, click on the “Connect” button. Information on connection establishment will be displayed.

If the DOUBLE CALL option is enabled in the control panel, select the “Double call” field before pressing the “Connect” button.

4. When the control panel goes off hook, connection will be established, of which you will be informed by the DLOADX program.

Initiating a modem connection from DLOADX program, with control panel calling back and making the call

Control panel settings:

- program the telephone number of modem connected to computer (PC PHONE NUMBER),
- enable ANSWERING – MODEM option (see: “Global options” p. 27),
- define the number of rings after which the control panel will answer incoming calls – RINGS BEFORE ANSWER (see: “Other global parameters” p. 31),
- enable the DOUBLE CALL option if the control panel is to answer only after the second call (see: “Global options” p. 27),
- configure the telephone communicator options (see: “Global options” p. 27).

DLOADX program settings:

- program the telephone number of control panel,
- configure the modem communication parameters.

1. Click on the  button in DLOADX program main menu. A drop down menu will be displayed.
2. Click “Modem 300bps”. Window with modem initialization information will be displayed.
3. After modem initialization, click on the “Connect” button. Information on connection establishment will be displayed.

If the DOUBLE CALL option is enabled in the control panel, select the “Double call” field before pressing the “Connect” button.

4. The control panel will receive the call, but will hang up. The DLOADX program will inform you that the control panel will call back.
5. The control panel will call back the number of computer modem. The DLOADX program will receive the call automatically or the program operator must accept establishing communication (which depends on DLOADX settings).

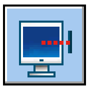
Initiating a modem connection by control panel

Control panel settings:

- program the telephone number of modem connected to computer (PC PHONE NUMBER),
- configure the telephone communicator options (see: “Global options” p. 27).

DLOADX program settings:

- configure the modem communication parameters.

1. Click on the  button in DLOADX program main menu. A drop down menu will be displayed.
2. Click “Modem 300bps”. Window with modem initialization information will be displayed.
3. Ask the user to start the START DWNLTEL function (he is supposed to enter the code and press [*], and then press in turn [0] [1] [#]). The control panel will call the computer modem number.
4. The DLOADX program will receive the call automatically or the program operator must accept establishing communication (which depends on DLOADX settings).

3.4.2 Programming over Ethernet

Communication via Ethernet can be established in one of the following methods:

1. Connection initialized from the DLOADX program. The control panel can be programmed from any location. If communication takes place in a wide area network, the Ethernet module must have a public IP address.
2. Connection initialized by the control panel. The control panel can be programmed only from specified location. This method should be used, when the system user does not want remote programming to take place without his knowledge. If communication takes place in a wide area network, the computer with DLOADX program must have a public IP address.
3. Establishing connection via the SATEL server. The control panel can be programmed from any location. No public IP address is required for the Ethernet module or the computer with DLOADX program.

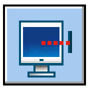
Initiating an Ethernet connection from DLOADX program

Ethernet module settings (see: “Ethernet module” p. 51):

- enable DLOADX->ETHM-1 CONNECTION option,
- program the number of TCP port which will be used for communication and the data encryption key,
- configure the Ethernet module.

DLOADX program settings:

- program the Ethernet module address,
- program the number of TCP port which will be used for communication and the data encryption key (or select the “LAN: ETHM-1” parameter set – the data programmed in settings of Ethernet module will be used).

1. Click on the  button in DLOADX program main menu. A drop down menu will be displayed.
2. Click “TCP/IP: DLOADX -> ETHM” (if you have programmed both sets of parameters for communication via the Ethernet network, when you hover mouse over “TCP/IP: DLOADX -> ETHM”, you can select “LAN/WAN” or “LAN”). The “Connection TCP/IP: DLOADX->ETHM-1” window will be displayed.
3. Click on the “Connect” button in the “Connection TCP/IP: DLOADX->ETHM-1” window. Connection establishment information will be displayed.
4. When communication is established, the DLOADX program will inform you about it.

Initiating an Ethernet connection by the control panel

Ethernet module settings (see: “Ethernet module” p. 51):

- program the address of the computer with DLOADX program, the number of TCP port which will be used for communication and the data encryption key,
- configure the Ethernet module.

DLOADX program settings:

- program the number of TCP port which will be used for communication and the data encryption key (or select the “LAN: ETHM-1” parameter set – the data programmed in settings of Ethernet module will be used).

1. Click on the  button in DLOADX program main menu. A drop down menu will be displayed.
2. Click “TCP/IP: DLOADX <- ETHM”. The “Connection TCP/IP: DLOADX<-ETHM-1” window will be displayed.
3. Ask the user to start the function ETHM-1→DLOADX (he is supposed to enter the code and press [*], and then press in turn [0] [7pqrs] [#]). The control panel will connect to the computer network address.
4. When communication is established, the DLOADX program will inform you about it.

Communication via the SATEL server

Ethernet module settings (see: “Ethernet module” p. 51):

- enable DLOADX->ETHM-1 CONNECTION and SATEL SERVER options,
- program the data encryption key.

DLOADX program settings:

- enter the individual identification number of the Ethernet module for the purpose of communication via the SATEL server,
- enter the MAC address of Ethernet module,
- program the data encryption key.

1. Click on the  button in DLOADX program main menu. A drop down menu will be displayed.
2. Click “TCP/IP: Satel server”. The “Connection TCP/IP: DLOADX<->ETHM-1” window will be displayed.
3. Click on the “Connect” button in the “Connection TCP/IP: DLOADX<->ETHM-1” window. Connection establishment information will be displayed.
4. When communication is established, the DLOADX program will inform you about it.

4. Global parameters

4.1 Programming the global parameters

You can program the global parameters:

- DLOADX program: “Global parameters” window.
- keypad: functions available in the GLOBAL PARAM. submenu (SERVICE MODE ▶3. GLOBAL PARAM.).

4.2 Global options

Reporting – TELEPHONE – if the option is enabled, the control panel can send event codes to the monitoring station by means of the telephone line.

Reporting – ETHM – if the option is enabled, the control panel can send event codes to the monitoring station over Ethernet.

Telephone messaging – if the option is enabled, the control panel can notify about the occurrence of specific events by means of voice or text messages using the phone communicator.

Answering – modem – if the option is enabled, external initiation of the modem communication with the control panel is possible.

Double call – if the option is enabled, you must call the control panel twice to be connected. The first time, wait for the preset number of rings and then hang up. Then call again within three minutes and the control panel will answer the call immediately. This solution makes it possible to connect after the control panel some additional devices which will be activated after a preset number of rings (e.g. answering machine, fax, etc.).

Tone dialing – if the option is enabled, the control panel will tone dial the telephone numbers (pulse dial, if this option is disabled).

Pulse 1/1.5 (off 1/2) – this option applies to pulse dialing. Before you enable it, make yourself familiar with the valid standard of pulse dialing.

No dial tone test – if the option is enabled, the control panel will not perform the test for dial tone before dialing the number and will start dialing the number 5 seconds after going "off hook". This makes it possible for the control panel to dial the number when some non-standard tones occur on the telephone line after going off hook (e.g. interrupted tone). When this option is disabled, the control panel will start dialing the number 3 seconds after going off hook, provided that the dial tone is present.

No answer tone test – if the option is enabled:

voice messaging: the voice message is played back 8 (first round) or 16 (next rounds) seconds after completion of number dialing (the control panel does not check whether the line is off-hook),

reporting: the control panel will ignore any signals (including the busy tone) received from the telephone exchange after dialing the telephone number, and will wait for the handshake from the monitoring station.

Enable this option if, after dialing the number, non-standard signals are received from the telephone exchange or in case of very poor quality connections.

Store keyfob events – if the option is enabled, using the keyfob is written into the event log.

Trouble memory until review – if the option is enabled, the trouble memory is being signaled until it is cleared (clearing the trouble memory is possible when you quit the 7. SYSTEM STATE user function).

Grade 2 – if the option is enabled, the system operates in accordance with the EN 50131 standard requirements for Grade 2, i.e.:

- the way of informing the users about the system state by means of LEDs, display and beeps in the keypads meets the requirements of the standard (see: USER MANUAL),
- the quick arming from keypad (without entering the code) is not available,
- new codes in the system must be composed of at least 5 characters,
- prior to arming, the control panel checks that no circumstances have occurred that prevent arming (ref. PREVENT ARMING IF NOT READY global option),

- in case of arming by means of the LCD keypad, the control panel will check if there are any zones bypassed in the partition – information on the bypassed zones is presented, if the user has the INSPECTION right,
- the warning alarm feature is enabled in the system (see: WARNING ALARM global option),
- the warning alarm is signaled at the 2. INTERNAL SIREN function output (ref. WARNING ALARM ON INTERNAL SIRENS global option).

You can enable/disable the option in keypad: SERVICE MODE ▶2. HARDWARE ▶1. KPDS & EXPS. ▶4. OPTIONS ▶GRADE2.

Serial data on OUT 3/4 – if the option is enabled, OUT3 and OUT4 outputs send the system status data (zone alarms, fire alarms, troubles, armed modes, etc.) and do not execute any other programmed functions. The outputs may be used to control the NR2-DSC radio monitoring transmitter (NEMROD system – PC-16 OUT format), made by NOKTON.

OUT 3/4 data extended mode – if the option is enabled, the OUT3 and OUT4 outputs will send the system status data in the form of frames (PC-16 OUT UA format). The option is available, if the SERIAL DATA ON OUT 3/4 option is enabled.

Arm./Disarm./Clear. signaling from zones only – if the option is enabled, outputs with the functions 1. EXTERNAL SIREN and 2. INTERNAL SIREN with enabled ARM/DISARM/CLEAR SIGN. option will signal only:

- starting of the arming procedure by zone or by means of keyfob,
- no possibility of arming (see: PREVENT ARMING IF NOT READY option or GRADE 2 option), if the arming command has been sent from keyfob,
- failed attempt of arming by means of keypad or keyfob (see: PREVENT ARMING IF NOT READY option or GRADE 2 option),
- disarming by zone or by means of keyfob,
- alarm clearing by zone or by means of keyfob.

Starting the arming procedure, disarming or alarm clearing by means of keypad, proximity card arm/disarm device or timer are not signaled.

Clear messaging on alarm clearing – if the option is enabled, clearing the alarm will automatically cancel messaging about this alarm, if the user clearing the alarm has the TEL. MESS. CLEARING right.

Service message after tamper alarm – if the option is enabled, information on the tamper alarm can only be cleared from the troubles memory by using the service code. In the LCD keypad, the “System tamper, call service” message will be displayed after the tamper alarm (unless the alarm messages are displayed). The message will no longer be displayed after the troubles memory is reset by the service.

Warning alarm – if the option is enabled, the warning alarm feature is enabled. It purpose is to delay the loud signaling and reporting, if any mistakes are made when entering the protected facility. The warning alarm is not reported. It can be signaled on the keypad, proximity card arm/disarm device or outputs with the function 2. INTERNAL SIREN. The warning alarm is triggered by the following zone types:

- 0. ENTRY/EXIT or 1. ENTRY/EXIT FINAL – unless the system is disarmed before completion of the ENTRY DELAY countdown,
- 2. ENTRY/EXIT ROUTE – if it is violated during the ENTRY DELAY countdown, and the system is not disarmed before completion of the DELAY TIME countdown,
- 3. INSTANT – if it is violated during the ENTRY DELAY countdown.

The warning alarm lasts 30 seconds. Unless the alarm system is disarmed during this time, the alarm will be triggered by the zone.

Warning alarm on internal sirens – if the option is enabled, the warning alarm will be signaled on outputs with the 2. INTERNAL SIREN function. The option is available, if the WARNING ALARM option is enabled.

Tamper alarm always audible – if the option is enabled, the tamper alarm will be signaled always on outputs with the 1. EXTERNAL SIREN and 2. INTERNAL SIREN functions (if the option is disabled, only in armed mode). Also, lack of the expander is always saved in the event log as a tamper alarm. If the option is disabled, lack of the expander will be saved in the event log:

– as a trouble, if the partition to which the expander is assigned, is disarmed (but the keypad will signal tamper alarm anyway),

– as a tamper alarm, if the partition is armed.

Tamper alarm on internal sirens – if the option is enabled, the tamper alarm will be signaled always on outputs with the 2. INTERNAL SIREN function (in armed mode only if the option is disabled). Additionally, the output will always signal lack of the expander (also when the event is logged as a trouble – see: TAMPER ALARM ALWAYS AUDIBLE option).

Block after 3 unknown codes/cards – if the option is enabled, after entering an incorrect code / reading in an incorrect card three times, the keypad / proximity card arm/disarm device will be blocked for 90 seconds. After this period of time has expired, each subsequent entry of an incorrect code / read-in of an incorrect card will block the keypad / proximity card arm/disarm device at once. The counter of incorrect codes / cards will be reset after a correct code is used.

Service Mode from RESET pins – if the option is enabled, it is possible to start the service mode and local programming "from pins". You can enable/disable the option in keypad: SERVICE MODE ▶0. SRVMOD CONFIG ▶6. SRVMOD OPT. ▶SRVMOD VIA RESET.

Limit storing "Test transm." events – when the option is enabled, if the "Test transmission" events directly follow one another, they are only written to the event log 3 times. Information on sending next test transmissions is not recorded. Any other event occurring in the system will reset the counter, i.e. it will be possible to log next three consecutive test transmissions.

Backlight off on AC loss – when the option is enabled, the backlighting in keypads is automatically switched off in case of 230 VAC power loss.

Answering/remote control when armed partition 1 / 2 – if the option is enabled, telephone answering and remote control features are only available when selected partitions are armed.

Additionally, the list of global options in the keypad includes:

– *TMP ALARM IN P.2 – alarm from the mainboard TMP zone is signaled in partition 2. In the DLOADX program, the partition in which alarm from TMP zone will be signaled is to be selected in the "VERSA – Structure" window, "Hardware" tab, after clicking on the system name on the left side,*

– *EVENTS LIMITAT., EXP. RESTART. REP., REST. AFT. BELL and REST. AFT. DISARM. – options available in the DLOADX program, "VERSA – Reporting" window, and described in section "Reporting parameters and options" (p. 70).*

4.3 Global times

Keypad's alarm time – time period during which alarm is signaled in keypads and proximity card arm/disarm devices. Up to 255 seconds can be programmed. Programming the value 0 means that the KEYPAD'S ALARM TIME will be 3 seconds.

No armed indication after – time counted from the moment of partition arming, after expiry of which the keypad LED indicating the partition armed status will go out. Up to 255

seconds can be programmed. Programming the value 0 means that the LED will be lit as long as the partition is armed.

AC loss report delay – time during which the control panel must be without AC power before the AC power trouble is saved to the event log and reported to the monitoring station. You can program up to 255 minutes. If you program 0, AC power trouble will neither be saved to the event log nor reported to the monitoring station.

Tel. line loss report delay – time during which abnormal voltage must be on the telephone line for the control panel to report the telephone line trouble. This delay prevents the reporting of short-time voltage dips (e.g. during a phone call) or decays. The delay can be up to 255 minutes. If you program 0, the control panel will not report the telephone line trouble.

RTC clock correction – if the accuracy of control panel clock is inadequate, the clock settings may be adjusted once per 24 hours (at midnight) by a defined time. The maximum correction can be ±19 seconds per 24 hours.

Summer/winter time – the control panel can automatically adjust the clock settings due to a change from the summer time to the winter time and vice versa. The following correction schemes are available:

- no correction,
- according to the European Union rules,
- according to the United States' rules,
- correction by 1 hour according to dates,
- correction by 2 hours according to dates.

Summer time from / Winter time from – if the control panel clock is to be corrected by 1 or 2 hours according to dates, you should enter the dates (day, month) after the clock is changed to the summer time (moved forward) or to the winter time (moved back).

4.4 Arming

Prevent arming if not ready – when the option is enabled, if the user arm the system by means of keypad or keyfob, the control panel checks that there are no circumstances that prevent the arming:

- a zone with PRIORITY option is violated in the partition which is to be armed,
- the 3. INSTANT, 4. DOUBLE KNOCK, 5. 24H BURGLARY, 6. 24H TAMPER, 7. 24H PANIC, 8. 24H PANIC SILENT, 9. 24H MEDICAL or 10. 24H FIRE type zone is violated in the partition which is to be armed,
- there is a trouble in the system.

If one of the aforementioned situations takes place, the control panel will not start the arming procedure (the LCD keypad enables forced arming – see: USER MANUAL). If none of the conditions is met, the control panel will start the arming procedure, but at the end of the exit delay countdown it will check again if the arming is possible (the quick arming being an exception). A violated zone or a trouble mean that the arming is not possible (i.e. the arming procedure will fail).

Additionally, when the option is enabled and the user has the INSPECTION right, the LCD keypad will inform, prior to arming, that there are bypassed zones in the partition (it does not apply to the quick arming).

You can enable/disable the option in keypad: SERVICE MODE ▶2. HARDWARE ▶1. KPDS & EXPS. ▶4. OPTIONS ▶ADVANCED ARMING.

Arm even if not ready after exit delay – if the option is enabled, a zone violation or trouble found at the end of exit delay countdown does not affect the arming procedure – the system will be armed. You can enable/disable the option in keypad: SERVICE MODE

▶2. HARDWARE ▶1. KPDS & EXPS. ▶4. OPTIONS ▶ARM EXDLY W.TRBL. The option is available, when the PREVENT ARMING IF NOT READY or GRADE 2 option is enabled.

4.5 Other global parameters

Rings before answer – number of rings after which the control panel will answer the incoming call. In the keypad, you can program this parameter: SERVICE MODE ▶7. ANSWERING ▶1. RINGS TO ANS.

User code min. lenght – the minimum number of characters required for the control panel to accept a new code or a changed code. This parameter will be included when creating and editing the codes (it is irrelevant to the codes already existing in the system).

5. Partitions

The partition is a separated area within the premises protected by the security alarm system. The subdivision into partitions enables arming/disarming the system only in part of the protected area, as well as limiting access to some portion of the premises to selected users. You can create 2 partitions.

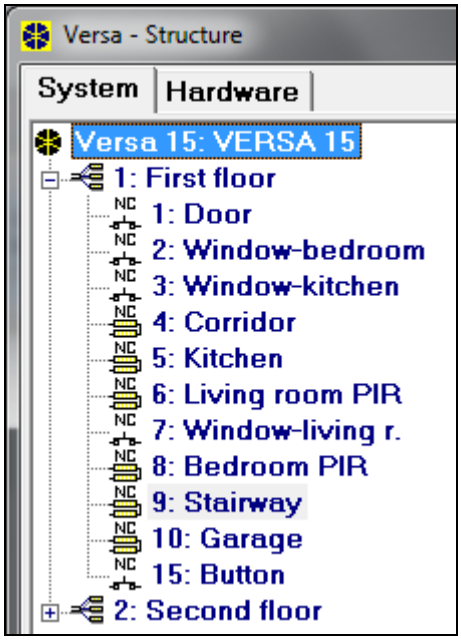


Fig. 6. DLOADX program: list of partitions and zones in a tree-like form in the “System” tab, “VERSA – Structure” window.

5.1 Configuring the partitions

You can configure the partitions as follows:

- DLOADX program: “VERSA – Structure” window →“System” tab. Partitions and zones are presented in the form of tree structure on the left side of the window (Fig. 6). Click on the partition you want to configure.
- keypad: functions available in the PARTITIONS submenu (SERVICE MODE ▶1. PARTITIONS).

5.2 Partition parameters

Name – individual name of the partition (up to 16 characters).

Partition exit delay – the time counted from the moment of starting the partition arming procedure which enables the protected area to be left without triggering an alarm. Violation of the 0. ENTRY/EXIT, 1. ENTRY/EXIT FINAL, 2. ENTRY/EXIT ROUTE or 4. DOUBLE KNOCK type zones during the exit delay time will trigger no alarm. Up to 255 seconds can be programmed.

The exit delay countdown can be terminated by means of the 1. ENTRY/EXIT FINAL or 16. EXIT DELAY TERMINATOR type zones.

Using the keypad, you can arm the system without the exit delay, if the hold down the key which ends the arming sequence (, or) for approx. 3 seconds.

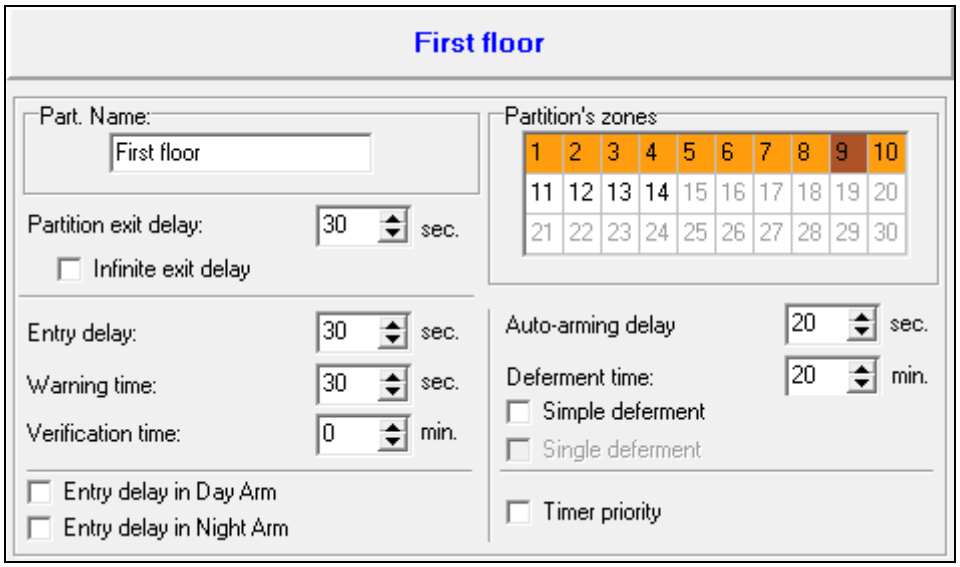


Fig. 7. DLOADX program: configuring partition parameters in the "VERSA – Structure" window.

Infinite exit delay – if the option is enabled, the partition exit delay can only be ended by means of the 1. ENTRY/EXIT FINAL, 16. EXIT DELAY TERMINATOR or 17. SHUNT LOCK type zones. If the exit delay countdown is not completed, the armed mode will not be activated (only the 3. INSTANT type zones will be armed).

Entry delay – the time counted from the moment of entry into the protected area which enables the partition to be disarmed before triggering an alarm. This parameter applies to the 0. ENTRY/EXIT and 1. ENTRY/EXIT FINAL type zones. The delay programmed for the partition is taken into account in case of the zones for which the value 0 has been individually programmed. The delay is programmed in seconds. Up to 255 seconds can be programmed. If the value 0 is programmed, the zone will act as an instant one.

Warning time – the time of warning alarm signaling for the partial armed mode (see: WARNING IN PARTIAL ARMING zone option). The time is programmed in seconds. Up to 255 seconds can be programmed. If the value 0 is programmed, the WARNING TIME will be 30 seconds. After expiry of the WARNING TIME, unless the partition is disarmed, the burglary alarm will be triggered.

The WARNING TIME parameter does not apply to the time of signaling the warning alarm which is generated when mistakes are made when entering into the protected object (see: WARNING ALARM global option).

Verification time – programming a value different from 0 means activating the alarm verification feature in the partition. Subject to verification are alarms from 0 to 5 type zones. The VERIFICATION TIME runs from the moment of alarm being triggered by such

a zone. If during the VERIFICATION TIME an alarm is triggered by another zone in the partition, programmed as 0 to 5 type, the control panel will report a verified alarm. The time is programmed in minutes. Up to 255 minutes can be programmed.

Entry delay in Day Arm – with this option enabled, after partition is armed in day mode with no delay, the entry delay time remains valid (there is only no exit delay time). With this option disabled, after partition is armed with no delay, there is neither exit delay nor entry delay time.

Entry delay in Night Arm – with this option enabled, after partition is armed in night mode with no delay, the entry delay time remains valid (there is only no exit delay time). With this option disabled, after partition is armed with no delay, there is neither exit delay nor entry delay time.

Auto-arming delay – the time counted from the moment when the timer is to arm the partition, enabling the arming to be deferred. The delay time is programmed in seconds. Up to 255 seconds can be programmed. Programming the value 0 means that the arming deferment will be unavailable.

Deferment time – the time by which the user can defer arming by the timer. The time is programmed in minutes. Up to 255 minutes can be programmed. Programming the value 0 means that the arming deferment will be unavailable.

Simple deferment – if the option is enabled, the user can defer auto-arming by pressing the ✖▼ key twice during the auto-arm delay time countdown.

Single deferment – if the option is enabled, the user can only use the simple deferment once, so as to postpone the auto-arming. Subsequent arming deferments are only possible by using the A-ARM DEFER. user function ([CODE] ✱ ▶6. SETTINGS ▶1. A-ARM DEFER.).

Timer priority – if this option is enabled, the timer always disarms the system (if the option is disabled, the timer will only disarm the system, if it armed it).

6. Zones

A zone can be assigned to one or two partitions. If the zone is assigned to two partitions, it can be armed when both partitions are armed or one of them only.

The system supports the following zones:

- hardwired – on the control panel PCB and in expanders. The number of available hardwired zones is determined by the control panel during the identification procedure.
- wireless – after connecting MICRA wireless system controller (VERSA-MCU) or the ABAX 2 (ACU-220 / ACU-280) / ABAX wireless system controller (ACU-120, ACU-270, ACU-100 or ACU-250). The number of available wireless zones depends on the number of wireless devices registered in the system and is determined during the procedure of adding them.
- virtual – zones which do not physically exist, but are controlled by means of keyfobs.

6.1 Programming the EOL resistor values

For the zones on the control panel mainboard and in zone expanders identified by the control panel as CA-64 Ei and CA-64 EPSi, the value of end-of-line resistors is programmable within the range from 500 Ω to 15 kΩ.

You can define the resistor value for the control panel zones:

- DLOADX program: “VERSA – Structure” window →“Hardware” tab →*[main board]*,
- keypad: SERVICE MODE ▶2. HARDWARE ▶5. EOL 1 RESIST. / ▶6. EOL 2 RESIST.

You can define the resistor value for the expander zones when configuring the expander:

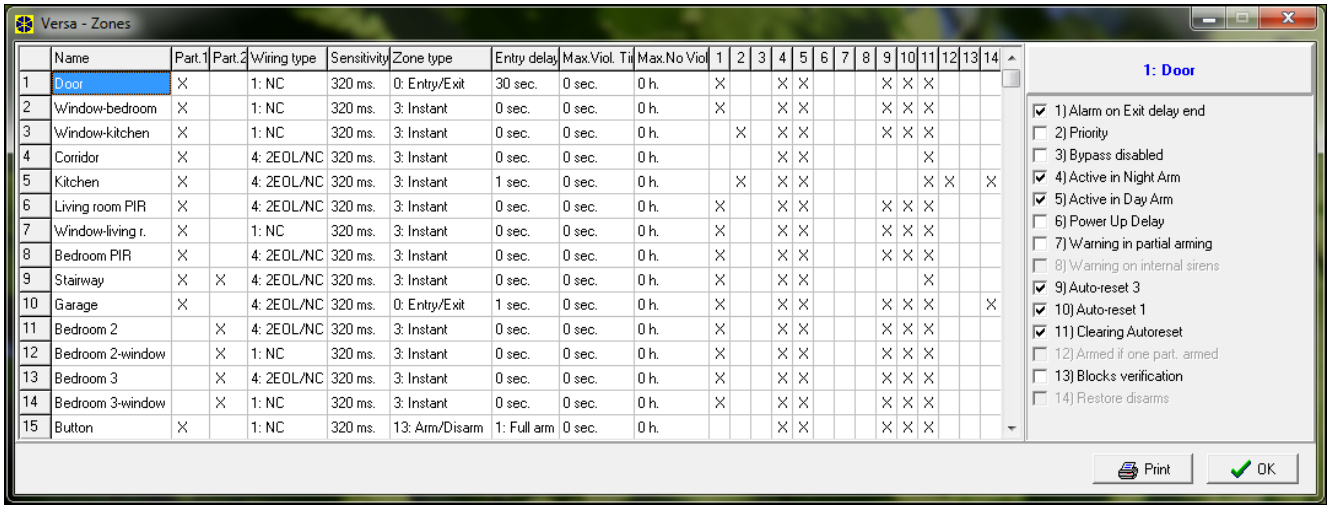
- DLOADX program: “VERSA – Structure” window →“Hardware” tab →“Expansion modules” branch →*[expander name]*,
- keypad: SERVICE MODE ▶2. HARDWARE ▶1. KPDS & EXP. ▶2. SETTINGS ▶*[expander name]*.

The sum of values programmed for the resistors R1 and R2 may not be lower than 500 Ω or higher than 15 kΩ.

You can program the value 0 for the resistor R2. In the 2EOL configuration you must use then two resistors, the resistance value of each being equal to half the value defined for the resistor R1.

In the EOL configuration, the resistance value is equal to the sum of values programmed for the resistors R1 and R2.

6.2 Configuring the zone parameters and options



	Name	Part.1	Part.2	Wiring type	Sensitivity	Zone type	Entry delay	Max.Viol. Ti	Max.No Viol	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Door	X		1: NC	320 ms.	0: Entry/Exit	30 sec.	0 sec.	0 h.	X			X	X				X	X	X			
2	Window-bedroom	X		1: NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X				X	X	X			
3	Window-kitchen	X		1: NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.		X		X	X				X	X	X			
4	Corridor	X		4: 2EOL/NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.				X	X						X			
5	Kitchen	X		4: 2EOL/NC	320 ms.	3: Instant	1 sec.	0 sec.	0 h.		X		X	X						X	X		X
6	Living room PIR	X		4: 2EOL/NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X				X	X	X			
7	Window-living r.	X		1: NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X				X	X	X			
8	Bedroom PIR	X		4: 2EOL/NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X				X	X	X			
9	Stairway	X	X	4: 2EOL/NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X						X			
10	Garage	X		4: 2EOL/NC	320 ms.	0: Entry/Exit	1 sec.	0 sec.	0 h.	X			X	X				X	X	X			X
11	Bedroom 2		X	4: 2EOL/NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X				X	X	X			
12	Bedroom 2-window		X	1: NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X				X	X	X			
13	Bedroom 3		X	4: 2EOL/NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X				X	X	X			
14	Bedroom 3-window		X	1: NC	320 ms.	3: Instant	0 sec.	0 sec.	0 h.	X			X	X				X	X	X			
15	Button	X		1: NC	320 ms.	13: Arm/Disarm	1: Full arm	0 sec.	0 h.				X	X				X	X	X			

Fig. 8. DLOADX program: “VERSA – Zones” window.

Parameters and options of the zones you can program:

- DLOADX program:
  - “VERSA – Structure” window →“System” tab. Partition and zones are presented in the tree-like form on the left-hand side of the window (Fig. 6). Click on the zone, the parameters and options of which you want to configure.
  - “VERSA – Zones” window (Fig. 8).
- keypad: ZONES function (SERVICE MODE ▶2. HARDWARE ▶2. ZONES). The programming is performed using the “step by step” method (see: p. 6):
  1. Zone selection.
  2. EOL type.
  3. Sensitivity [wiring type NO, NC, EOL and 2EOL].
  4. Pulse validity [only for ROLLER wiring type].
  5. Pulses count [only for ROLLER wiring type].
  6. Sensitivity [only for VIBRATION wiring type].
  7. Pulses count [only for VIBRATION wiring type].
  8. Zone type.

9. Alarm delay [ARM MODE for 13. ARM/DISARM and 14. ARMING type zones, and the EVENT for the 19. TROUBLE type zone].
10. Max. violation time.
11. Max. no violation time.
12. Zone options.
13. Zone name [only in LCD keypad].

6.3 Zone parameters

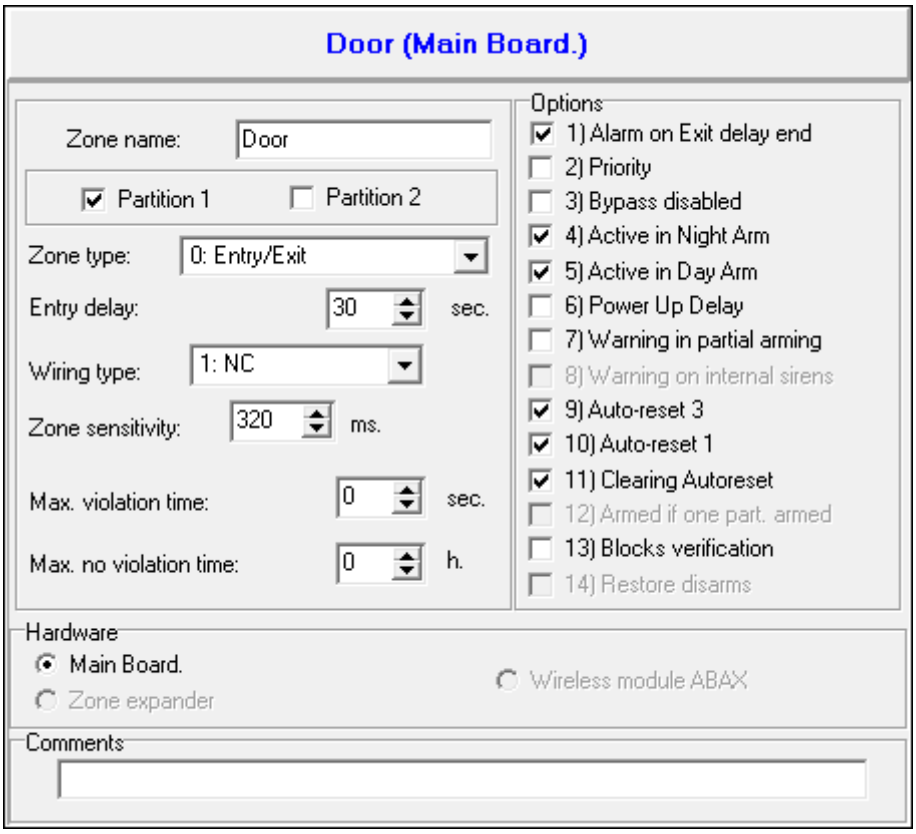


Fig. 9. DLOADX program: programming the zone parameters in "VERSA – Structure" window.

Zone name – individual name of zone (up to 16 characters).

Partition 1 / **Partition 2** – partition to which the zone is assigned. The zone must be assigned at least one partition, for its status to be supervised.

Entry delay – the time counted from the moment of violating the 0. ENTRY/EXIT or 1. ENTRY/EXIT FINAL type zone, which makes disarming possible before triggering the alarm. Up to 255 seconds can be programmed. If the value 0 is programmed, the ENTRY DELAY programmed for the partition will be taken into account. If the value 0 is programmed for both the zone and the partition, the zone will act as an instant one.

Delay – the time counted from the moment of violating the 2. ENTRY/EXIT ROUTE type zone, if it acts as a delayed one. Up to 255 seconds can be programmed. If the value 0 is programmed, the ENTRY DELAY programmed for the partition will be treated as the DELAY TIME. If the value 0 is programmed for both the zone and the partition, the zone will act as an instant one.

Delay activation time – the time counted from the moment of violating the 18. ENTRY ROUTE ENABLING type zone. During countdown of this time, the 2. ENTRY/EXIT ROUTE type zone will act as the delayed ones. Up to 255 seconds can be programmed. If the value 0 is

programmed, the ENTRY DELAY programmed for the partition will be treated as the DELAY ACTIVATION TIME. If the value 0 is programmed for both the zone and the partition, violation of the zone will have no effect.

Waiting time – the time counted from the moment of violating the 4. DOUBLE KNOCK type zone. If the zone is violated again during the waiting time, it will trigger alarm. Up to 255 seconds can be programmed. Programming the value 0 means that the WAITING TIME will be 30 seconds.

In the LCD keypad, the ENTRY DELAY, DELAY ACTIVATION TIME and WAITING TIME parameters are programmed as the ALARM DELAY.

Arm mode – the armed mode activated after violating the 13. ARM/DISARM or 14. ARMING type zone. You can select either fully arming, day arming or night arming.

Event – number of the event that will be written into the control panel memory and can be reported to the monitoring station upon violation of the 19. TROUBLE type zone. You can enter the following values for the corresponding codes of alarm events:

1 – 201 Low water pressure

2 – 202 Low CO2

3 – 203 Gate valve sensor

4 – 204 Low water level

5 – 205 Pump activated

6 – 206 Pump failure

51 – 151 Gas detected

52 – 152 Refrigeration

53 – 153 Loss of heat

54 – 154 Water leakage

55 – 155 Foil break trouble

56 – 156 Day trouble

57 – 157 Low bottle gas level

58 – 158 High temperature

59 – 159 Low temperature

61 – 161 Loss of air flow

62 – 162 Carbon monoxide (CO) detected

63 – 163 Tank level trouble

Entering a different value means that the zone violation will trigger the trouble signaling, but no alarm events from zone will be written to the event log.

Wiring type – type of detector and the method of its connection (zone configuration):

no detector – no detector is connected to the zone,

NC – the zone supports a detector of NC (normally closed) type,

NO – the zone supports a detector of NO (normally open) type,

EOL – the zone supports a detector of NO or NC type with EOL resistor in the circuit,

2EOL/NO – the zone supports a detector of NO type with two EOL resistors in the circuit,

2EOL/NC – the zone supports a detector of NC type with two EOL resistors in the circuit,

roller – the zone supervise a roller shutter detector,

vibration – the zone supervise a shock detector (also NC type detector).

In case of the VIBRATION zone wiring, opening the circuit for 200 ms or longer – irrespective of the programmed number of pulses and sensitivity (see below) – will be

interpreted as violation. This solution enables a magnetic contact to be connected in series with the shock detector.

Sensitivity – depending on selected wiring type:

- **NO, NC, EOL and 2EOL** – the time during which the zone must be violated, so that it can be noted by the control panel. The sensitivity is programmed in milliseconds. Values from the 20 ms to 5100 ms range can be entered.
- **Vibration** – the shock whose duration is equal to or longer than the defined time will cause violation of the zone. Values from the 3 ms to 96 ms range can be programmed (every 3 ms).

Pulse validity – the time counted from the pulse occurrence during which subsequent pulses must occur (their number being defined as the PULSE COUNT) so that the zone is violated. The following values can be programmed: 30 s, 120 s, 240 s and 0. If no further pulses will occur within the defined time period, the pulse counter will be reset. The pulse counter is reset automatically at arming/disarming. If the value 0 is programmed, the counter will only be reset at arming/disarming. This parameter is programmed for the ROLLER zone wiring.

Pulse count – the number of pulses/shocks after which the zone will be violated. This parameter is programmed for the ROLLER and VIBRATION zone wiring. For the VIBRATION zone wiring, it is possible to program values from 0 to 7 (for the value 0, the pulses (shocks) will not be counted, the SENSITIVITY parameter only being taken into account). For the ROLLER zone wiring, you can program values from 1 to 8.

In the DLOADX program, all the required parameters for zones in ROLLER and VIBRATION configuration are programmed in the "Sensitivity" field.

Max. violation time – if the zone is violated for the preset time (e.g. because the detector is damaged or masked), a trouble will be reported. Up to 255 seconds can be programmed. Programming the value 0 means that the control panel will not check whether the zone is violated too long.

Max. no violation time – if zone is not violated for the preset time (e.g. because of damaging or masking the detector), a trouble will be reported. When the zone is armed, the countdown is not running. You can program up to 255 hours. Programming the value 0 means that the control panel will not check whether the zone is violated or not.

6.4 Zone types

0. ENTRY/EXIT – a delayed zone combining two functions:
entry – violation of the zone starts entry delay counting in the partition and turns on delay for the 2. ENTRY/EXIT ROUTE type zone.

exit – violation of the zone during exit delay countdown is equivalent to the partition exit.

1. ENTRY/EXIT FINAL – the same as the 0. ENTRY/EXIT type, but if the arming procedure has started and the control panel registers the zone restore, the exit delay countdown will be terminated.

2. ENTRY/EXIT ROUTE – during the countdown of ENTRY DELAY or DELAY ACTIVATION TIME the zone acts as a delayed one (alarm will be triggered after expiry of the DELAY TIME). In other situations it acts as an instant zone.

3. INSTANT – instant zone, which is already armed during exit delay countdown.

4. DOUBLE KNOCK – the zone triggers the burglary alarm only after the second violation. The first violation of the zone only results in the "Zone violation" event being logged (the event to may reported in format 4/2). The second violation must take place during the WAITING TIME countdown.

5. 24H BURGLARY – dedicated zone for the detectors which should be armed at all times (e.g. glass break detectors).

6. 24H TAMPER – dedicated, permanently armed zone for tamper circuits. Violation of the zone is additionally signaled as a trouble.

7. 24H PANIC – permanently armed zone, intended for operating the panic buttons.

8. 24H PANIC SILENT – permanently armed zone, intended for operating the panic buttons. Alarm from the zone is not signaled on keypads, proximity card arm/disarm devices and outputs, but the event code is sent to the monitoring station.

9. 24H MEDICAL – permanently armed zone for calling medical assistance.

10. 24H FIRE – dedicated, permanently armed zone for operating fire detectors.

11. DETECTOR MASK – permanently armed zone for antimasking control. Violation of the zone is interpreted by the control panel as a detector trouble.

12. NO ALARM ACTION – the zone may be used to control the output with function 13. ZONE VIOLATION, 15. CONTROLLED or 16. READY STATUS. An additional option enables the zone to be used for supervision of the key box (KEYBOX CONTROL option).

13. **ARM/DISARM** – the zone controls the arming status of the partition it belongs to. Violation of the zone starts the arming procedure or disarms the partition (depending on the current status of the partition).

14. ARMING – violation of the zone starts the procedure of arming the partition to which the zone belongs.

15. DISARMING – violation of the zone disarms the partition to which the zone belongs.

16. EXIT DELAY TERMINATOR – violation of the zone ends the partition exit delay countdown.

17. SHUNT LOCK – the zone ends the partition exit delay countdown and – depending on the BLOCKS VERIFICATION option – will disable verification or disarm the partition to which it belongs. The way of controlling (the zone violation / zone restore) is determined by the option RESTORE DISABLES VERIF. or RESTORE DISARMS.

18. ENTRY ROUTE ENABLING – violation of the zone activates delay for the 2. ENTRY/EXIT ROUTE type zones in the partition to which the zone belongs. The zones will act as delayed ones for the DELAY ACTIVATION TIME. After expiry of the time, unless the system is disarmed, the zones will again act as the instant ones. If the DELAY ACTIVATION TIME for a zone will be programmed as equal to 0, and at the same time the ENTRY DELAY programmed for the partition is equal to 0, violation of the zone will have no effect.

19. TROUBLE – violation of the zone is treated by the control panel as a trouble. Additionally, an alarm event may be written into the control panel memory (see: EVENT parameter).

6.5 Zone options

Alarm on exit delay end – when the option is enabled, if the zone is violated at the moment of ending the exit delay countdown, it will trigger an alarm (if this option is disabled, the zone will only trigger the alarm when the status changes from normal to violation during the armed mode).

Priority – if the option is enabled, arming is impossible when the zone is violated.

Bypass disabled – if the option is enabled, the user cannot bypass the zone.

Active in night arm – if the option is enabled, the zone is armed when the night armed mode is activated.

Active in day arm – if the option is enabled, the zone is armed when the day armed mode is activated.

Power-up delay – if the option is enabled, the zone is bypassed for 120 seconds after power supply is turned on (this will prevent triggering false alarms e.g. during start-up of the control panel).

Warning in partial arming – if the option is enabled and the partition is set to day or night arm mode, the zone will trigger a warning alarm. It can be signaled in the keypad, in the proximity card arm/disarm device or at the 2. INTERNAL SIREN function output. It is not reported to the monitoring station. If you do not disarm the system during the warning alarm, the zone will trigger a burglary alarm (see: parameter WARNING TIME p. 32).

Warning alarm in the partial armed mode will work irrespective of the WARNING ALARM global option, which refers to the delay of loud signaling and reporting if any mistakes are made when entering into the protected facility.

Warning on internal sirens – if the option is enabled, warning alarm in the partial armed mode is signaled on the output with the 2. INTERNAL SIREN function.

Signaling on internal sirens – option for the 19. TROUBLE zone type. If it is enabled, the zone violation is indicated on the internal sirens.

Auto-reset 3 – if the option is enabled, the zone can trigger up to 3 alarms. As long as the alarm is not cleared or the partition is not armed/disarmed, violations of the zone will not trigger any alarm.

Auto-reset 1 – if the option is enabled, the zone can trigger only 1 alarm. As long as the alarm is not cleared or the partition is not armed/disarmed, violations of the zone will not trigger any alarm.

If the AUTO-RESET 3 and AUTO-RESET 1 options are enabled at the same time, the AUTO-RESET 3 option will have priority.

Clearing Autoreset – if the option is enabled, the alarm counters for zones for which the AUTO-RESET 3 or AUTO-RESET 1 option is enabled will be automatically reset at midnight (violations of these zones will be able to trigger alarms again).

Armed if one part. armed – the option refers to the zones which are assigned to both partitions. If the option is enabled, the zone is armed when one of the partitions is armed. If the option is disabled, the zone is armed when both partitions are armed. The option is also available in the event of ubypassing zones during disarming (if the option is enabled, the zone will only be unbypassed after disarming both partitions).

Blocks verification – an option for the 0. ENTRY/EXIT, 1. ENTRY/EXIT FINAL and 17. SHUNT LOCK zone types. If it is enabled, the zone will block alarm verification in the partition:

– after the zone violation – the 0. ENTRY/EXIT and 1. ENTRY/EXIT FINAL zone types, and also the 17. SHUNT LOCK zone type, when the RESTORE DISABLES VERIF. option is disabled,

– after the zone restore – the 17. SHUNT LOCK zone type, when the RESTORE DISABLES VERIF. option is enabled.

In case of the 17. SHUNT LOCK zone type, the zone will disarm the system when the BLOCKS VERIFICATION option is disabled.

Restore disarms – an option for the 17. SHUNT LOCK zone type. If the option is enabled, the zone restore will disarm the partition to which the zone belongs, and the zone violation will shorten the exit delay time. If the option is disabled, the zone violation will disarm the partition, and zone restore will shorten the exit delay time. The option is available, if the BLOCKS VERIFICATION option is disabled.

Restore disables verif. – an option for the 17. SHUNT LOCK zone type. If the option is enabled, the zone restore will block verification in the partition to which the zone belongs, and the zone violation will shorten the exit delay time. If the option is disabled, the zone violation will block verification, and the zone restore will shorten the exit delay time. The option is available, if the BLOCKS VERIFICATION option is enabled.

Alarm clearing – an option for the 13. ARM/DISARM and 15. DISARMING zone types. If the option is enabled, together with disarming, the alarm is cleared (except for the tamper

alarms). Violation of the 15. DISARMING type zone will also clear the alarm, when the system is not armed.

Store to event log – an option for the 12: NO ALARM ACTION zone type. If the option is enabled, violation of the zone is saved into the event log (the way of saving the event depends on the KEYBOX CONTROL option).

Store event only if armed – an option for the 12: NO ALARM ACTION zone type. If the option is enabled, zone violations are saved in the event log when the partition to which the zone belongs is armed. The option is available when the STORE TO EVENT LOG option is enabled.

Keybox control – an option for the 12: NO ALARM ACTION zone type. If this option is enabled, violation of the zone will result in logging an event which informs that the keybox is open. The event code is sent to the monitoring station. If this option is disabled, an event will be logged informing about zone violation, which will not be reported. The option is available when the STORE TO EVENT LOG option is enabled.

LED	Name displayed on LCD keypad	Options	Zone types
1	Al.on exit end	Alarm on exit delay end	0-10
2	Priority	Priority	all
3	Bypass disabled	Bypass disabled	all
4	Active night arm	Active in night arm	0-4
5	Active day arm	Active in day arm	0-4
6	Power up delay	Power-up delay	all
7	Warn.in part.arm	Warning in partial arming	0-4
8	Warn.on int.sir.	Warning on internal sirens	0-4
		Signaling on internal sirens	19
9	Auto-bypass 3	Auto-reset 3	0-10, 19
10	Auto-bypass 1	Auto-reset 1	0-10, 19
11	Autobypass reset	Clearing Autoreset	0-10, 19
12	Arm.with one p.	Armed if one part. armed	0-4
		Keybox control	12
13	Disable verific.	Blocks verification	0, 1, 17
		Store to event log	12
14	Finish exit time	Restore disarms	17
		Restore disables verif.	17
		Store event only if armed	12
		Alarm clearing	13, 15

Table 5. The method of presenting zone options on keypads. In graphic mode, the options in the LCD keypad are numbered in the same way as in the LED keypad.

6.6 Hardware

Numbers of zones on the mainboard, in zone expanders and wireless system controllers may overlap. If the zone numbers overlap, the state of only one of them will be supervised. Select the zone that is to be supervised.

When using the DLOADX program, open the “VERSA – Structure” window, go to the “System” tab, click on the zone, and then select whether the zone on mainboard, in zone expander or wireless system controller is to be supervised.

When using the keypad:

- you can use the WIRELSS.ZONES function (SERVICE MODE ▶2. HARDWARE ▶1. KPDS & EXPS. ▶3. WIRELESS DEV. ▶4. WIRELSS.ZONES) to select whether a wireless or wired zone will be supervised. In the case of LCD keypad, the symbol next to the zone name has the following meaning: ▮ - wireless zone is supervised; · - wired zone is supervised. In the case of LED keypad, the LEDs designated by numbers (LED number corresponds to zone number) provide the following information: LED ON – a wireless zone is supervised; LED OFF – a wired zone is supervised.
- you can use the VERSA ZONES function (SERVICE MODE ▶2. HARDWARE ▶7. VERSA ZONES) to select the wired zone to be supervised. In the case of LCD keypad, the symbol next to the zone name has the following meaning: ▮ - zone on the mainboard is supervised; · - zone in the zone expander is supervised. In the case of LED keypad, the LEDs designated by numbers (LED number corresponds to zone number) provide the following information: LED ON – zone on the mainboard is supervised; LED OFF – zone in the zone expander is supervised.

7. Outputs

The system supports the following outputs:

- hardwired – on the control panel PCB and in the expander.
- wireless – after connection of the ABAX 2 (ACU-220 / ACU-280) / ABAX (ACU-120, ACU-270, ACU-100 or ACU-250) wireless system controller. The number of available wireless outputs depends on the number of wireless devices registered in the system and is determined during the procedure of adding them.

7.1 Configuring the outputs

You can configure the outputs as follows:

- DLOADX program: “VERSA – Outputs” window (Fig. 10).
- keypad: OUTPUTS function SERVICE MODE ▶2. HARDWARE ▶3. OUTPUTS). Programming is performed by means of the “step by step” method (see: p. 6):
  1. Select output.
  2. Output function.
  3. Cut-off time.
  4. Triggering zones [the partition armed mode is selected for the outputs with functions 18. ARMED STATUS and 20. ALARM/ARM STATUS, and the troubles for the output with function 19. TROUBLE STATUS (see: Section OUTPUT PARAMETERS)].
  5. Output options.
  6. Output name [only in LCD keypad].

7.2 Output functions

0. NOT USED

1. EXTERNAL SIREN – signals the burglary, panic and tamper alarms.

2. INTERNAL SIREN – signals the burglary, panic and tamper alarms, as well as the warning alarms.

i *The way of signaling the tamper alarms by the outputs with functions 1. EXTERNAL SIREN and 2. INTERNAL SIREN depends on the global options TAMPER ALARM ALWAYS AUDIBLE and TAMPER ALARM ON INTERNAL SIRENS.*

3. BURGLARY – signals the alarms from 0 to 5 type zones.

4. FIRE ALARM – signals the fire alarms from keypad and from 10. 24H FIRE type zones.

5. "DURESS" ALARM – signals that code with DURESS right was used for arming/disarming or alarm clearing.

6. PANIC ALARM – signals the panic alarms from keypad and from 7. 24H PANIC type zones.

7. AUX. ALARM – signals the medical assistance call alarms triggered from keypad and from 9. 24H MEDICAL type zones.

8. ALARM – NOT VERIFIED – signals the unverified alarms.

9. ALARM - VERIFIED – signals the verified alarms.

10. TAMPER ALARM – signals the tamper alarms.

11. FIRE DETECTORS POWER SUPPLY – the dedicated output for power supply of the fire detectors with automatic verification alarm. After violation of the fire zone the output will be disabled for 16 seconds. If, after the power is turned on again, another violation from the fire zone occurs, the fire alarm will be triggered.

12. POWER SUPPLY ON ARMED – the dedicated output for power supply of the detectors which should not be active when the system is disarmed. It gets activated at the moment of starting the arming procedure (the exit delay is not taken into account).

13. ZONE VIOLATION – signals violation of the zones.

14. CHIME – signals violation of the zones when they are disarmed.

15. CONTROLLED – controlled by means of zones, timers, keypad or from keyfob.

16. READY STATUS – indicates whether the system is ready for arming, i.e. whether there are no violated zones (active when there is no violation).

17. EXIT DELAY STATUS – indicates that the EXIT DELAY countdown is running.

18. ARMED STATUS – indicates the armed mode (after completion of the exit delay countdown).

19. TROUBLE STATUS – indicates troubles.

20. ALARM/ARM STATUS – indicates alarms (pulsating mode) and arm status (continuous mode – after end of the exit delay countdown).

21. DETECTORS RESETTING – dedicated output to control the alarm memory reset in detectors. Activated at the moment of starting the arming procedure (the exit delay is not taken into account). It can also be activated by using the OUTPUTS RESET user function.

22. ETHM TROUBLE STATUS – indicates Ethernet module troubles.

7.3 Output parameters

Output name – individual name of the output (up to 16 characters).

Cut-off time – time during which the alarm outputs and the outputs with functions 13. ZONE VIOLATION, 14. CHIME, 15. CONTROLLED and 21. DETECTORS RESETTING are active. Entering the value 0 modifies the way of functioning of some outputs:

- alarm outputs remain active until the alarm is cleared,
- the 13. ZONE VIOLATION output remains active throughout the time of zone violation (the PULSE option is disabled then),
- the 14. CHIME output remains active until deactivated by the OUTPUTS RESET user function,
- the 15. CONTROLLED output remains active until another violation of the controlling zone, disabling of timer or disabling of the output by means of keypad (bistable mode).

Activation: zones – the zones whose status has effect on the output status.

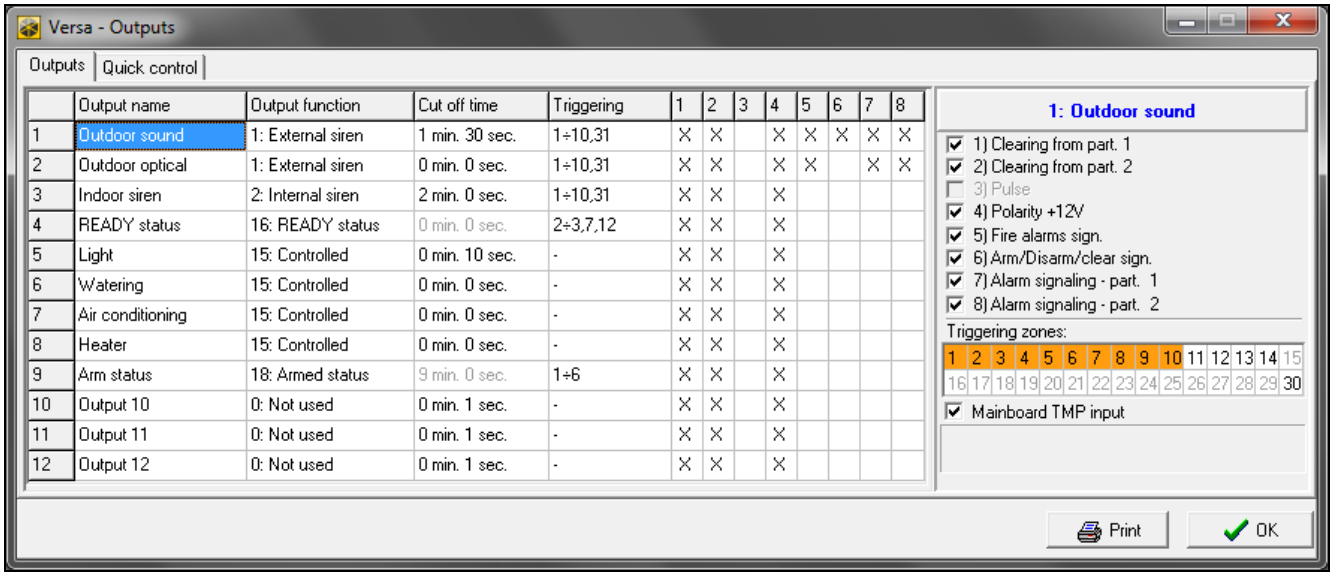


Fig. 10. DLOADX program: “VERSA – Outputs” window.

Activation: partition armed mode – the armed modes whose activation in the partition will activate the 18. ARMED STATUS or 20. ALARM/ARM STATUS output (the number corresponds to the LED number in the LED keypad and to the item number in graphic mode in the LCD keypad):

1. Partition 1 – full armed mode
2. Partition 1 – night armed mode
3. Partition 1 – day armed mode
4. Partition 2 – full armed mode
5. Partition 2 – night armed mode
6. Partition 2 – day armed mode

In case of the 20. ALARM/ARM STATUS function output, selecting any armed mode in a partition means that the output will signal alarms from that partition.

Activation: troubles – the troubles the occurrence of which will activate the output. For the 19. TROUBLE STATUS output function, these can be the following troubles (the number corresponds to the LED number in the LED keypad and to the item number in graphic mode in the LCD keypad):

1. AC loss – control panel mainboard
2. Battery trouble – control panel mainboard
3. Telephone line – no voltage
4. Telephone line – no dial tone
5. OUT1 output trouble
6. OUT2 output trouble
7. KPD output trouble
8. AUX output trouble
9. Reporting trouble – monitoring station 1
10. Reporting trouble – monitoring station 2
11. Wireless system jamming
12. Communication bus short circuit
13. Clock loss
14. RAM memory error

15. Mainboard TMP open
16. Zones – tamper
17. Zones – long violation
18. Zones – no violation
19. Zones – masking
20. Wireless device battery low
21. Wireless device communication loss
22. Module tamper
23. No presence (module)
24. AC loss (module)
25. Battery trouble (module)
26. Power output overload (module)
27. Low battery (keyfobs)
28. Module restart
29. Control panel restart

For the 22. ETHM TROUBLE STATUS output function, these can be the following troubles (the number corresponds to the LED number in the LED keypad and to the item number in graphic mode in the LCD keypad):

1. Reporting trouble – station 1 – ETHM
2. Reporting trouble – station 2 – ETHM
21. No Ethernet connection
22. No Ethernet connection (PING)
23. No connection to SATEL server
24. Wrong pair MAC/ID

7.4 Output options

Clearing from part. 1 / Clearing from part. 2 – depending on the output function:

- alarm outputs – the alarm can be cleared by users having access to the selected partition,
- the 1. EXTERNAL SIREN and 2. INTERNAL SIREN outputs with enabled ARM/DISARM/CLEAR SIGN. option – the output will be activated when in the selected partition the procedure of arming has been initiated, arming is not possible, armed mode is deactivated, or when alarm is cleared in it,
- 5. "DURESS" ALARM – the users having access to the selected partition can deactivate the output by means of the OUTPUTS RESET user function.

Partition 1 / Partition 2 – depending on the output function:

- 12. POWER SUPPLY ON ARMED – the output is active when the selected partition is armed (it activates after starting the arming procedure, without taking the exit delay into account),
- 15. CONTROLLED – the output can be controlled by the users having access to the selected partition by means of the user function CONTROL (if no partition is selected, the function CONTROL will not be available in the keypad),
- 17. EXIT DELAY STATUS – the output is active when the exit delay countdown is running in the selected partition,
- 21. DETECTORS RESETTING – the output activates for a preset time, when the arming procedure is initiated in the selected partition (without taking into account the exit delay).

The users authorized to access the given partition can activate the output by using the OUTPUTS RESET function.

Reset in partition 1 / **Reset in partition 2** – depending on the output function:

– 11. FIRE DETECTORS POWER SUPPLY – the users having access to the selected partition can deactivate the output for 16 seconds by means of the OUTPUTS RESET user function,

– 14. CHIME, for which the CUT-OFF TIME equal to 0 has been programmed – the users having access to the selected partition can deactivate the output by means of the OUTPUTS RESET user function.

Pulse – output with pulsating mode of operation (0.5/0.5 sec.). This option refers to the outputs for which the cut-off time is to be programmed (except for the 1. EXTERNAL SIREN and 2. INTERNAL SIREN outputs), and outputs with the 17. EXIT DELAY STATUS, 18. ARMED STATUS, 19. TROUBLE STATUS and 22. ETHM TROUBLE STATUS functions.

Polarity +12V – sets the output operating mode. If the option is disabled, the output is inverted.

	"–" terminal of high-current output / low-current output	
	option enabled (normal polarity)	**option disabled** (reverse polarity)
active state	shorted to ground	disconnected from ground
inactive state	disconnected from ground	shorted to ground

Table 6. Mode of output operation depending on the POLARITY +12V option.

Fire alarms sign. – option for the 1. EXTERNAL SIREN and 2. INTERNAL SIREN outputs. The output signals in pulsating mode the fire alarms from selected zones (see: ACTIVATION: ZONES) and partitions (see: ALARM SIGNALING – PARTITION 1 and ALARM SIGNALING – PARTITION 2 output options).

One partition sign. – option for the 18. ARMED STATUS and 20. ALARM/ARM STATUS outputs. The output indicates armed mode when any of the two partitions is armed (if the option is disabled, only when both partitions are armed).

Arm/Disarm/Clear sign. – option for the 1. EXTERNAL SIREN and 2. INTERNAL SIREN outputs (see also: CLEARING FROM PART. 1 and CLEARING FROM PART. 2 output options and ARM./DISARM./CLEAR. SIGNALING FROM ZONES ONLY global option). The output signals:

– starting the arming procedure (which is equivalent to arming if no exit delay has been programmed) – 1 tone,

– disarming – 2 tones,

– alarm clearing – 4 tones,

– denial of arming or arming procedure failure (see: PREVENT ARMING IF NOT READY global option or GRADE 2 global option) – 7 tones.

Tone duration is about 0.3 second.

Alarm signaling – part. 1 / Alarm signaling – part. 2 – an option for the alarm outputs. The output signals the selected partition alarms which were not triggered by zones.

Timer 1 / Timer 2 / Timer 3 / Timer 4 – options for the 15. CONTROLLED outputs. The output is controlled by selected timer (if timer status changes to "ON", the output will be activated for the CUT-OFF TIME).

Mainboard TMP input – an option for the 1. EXTERNAL SIREN, 2. INTERNAL SIREN and 10. TAMPER ALARM outputs. The output will be activated by the mainboard tamper (violation of the mainboard TMP zone).

LED	Name displayed on LCD keypad	Options	Output functions
1	Part.1 clears	Clearing from part. 1	1-10
		Partition 1	12, 15, 17, 21
		Reset in partition 1	11, 14
2	Part.2 clears	Clearing from part. 2	1-10
		Partition 2	12, 15, 17, 21
		Reset in partition 2	11, 14
3	Pulsation	Pulse	3-10, 13-15, 17-19, 22
4	Polarization +	Polarity +12V	all
5	Fire alarm	Fire alarms signaling	1, 2
		Timer 1	15
		One partition sign.	18, 20
6	Arm/dArm/Cl.chrp	Arm/Disarm/Clear sign.	1, 2
		Timer 2	15
7	Part.1 alarms	Alarm signaling – part. 1	1-10
		Timer 3	15
8	Part.2 alarms	Alarm signaling – part. 2	1-10
		Timer 4	15
9	31.TMP zone	Mainboard TMP input	1, 2, 10

Table 7. The way of presenting output options in keypads. The options in the graphic mode in the LCD keypad are numbered in the same way as in the LED keypad.

7.5 Quick control of outputs

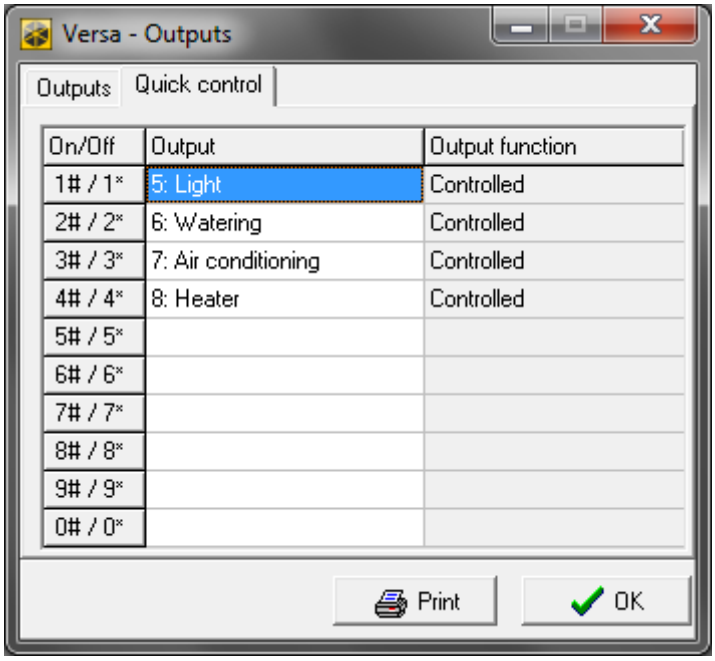


Fig. 11. DLOADX program: assigning the outputs to keypad keys.

If the quick control of the outputs 15. CONTROLLED is to be available in keypads, the outputs of this type must be assigned to the corresponding keypad keys. One output can be assigned to each of the keys designated with numerals.

8. Devices

You can connect to the control panel communication bus additional devices (keypads, expanders, other modules) which will be needed in the alarm system.

8.1 Configuring the devices

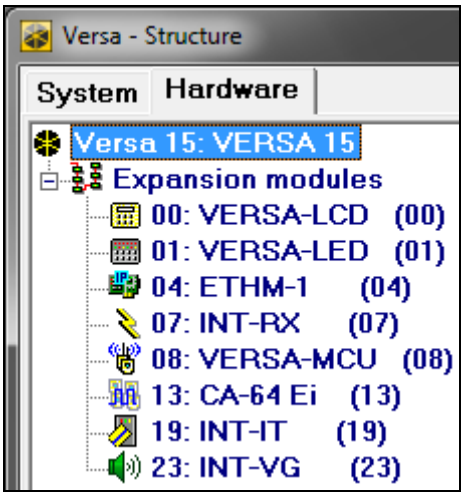


Fig. 12. DLOADX program: List of devices connected to the control panel, displayed in the "Hardware" tab, "VERSA – Structure" window.

You can configure the devices as follows:

- DLOADX program: "VERSA – Structure" window →"Hardware" tab. The list of devices is presented in the form of tree structure on the left side of the window (Fig. 12). Click on the name of device you want to configure.
- keypad: SETTINGS function (SERVICE MODE ▶2. HARDWARE ▶1. KPDS & EXPS. ▶2. SETTINGS). Programming is performed by means of the "step by step" method (see: p. 6). In the first step, select the device you want to configure.

The following can be programmed for all devices connected to the communication bus:

Name – individual name of the device (up to 16 characters).

Tamper signaled in part. – the partition in which tamper alarm will be triggered in the event of tamper or disconnection of the device from the system.

Descriptions displayed on LCD keypad are shown in square brackets.

8.2 Keypad

8.2.1 Parameters and options

Descriptions displayed on LCD keypad are shown in square brackets.

CHIME signal of zones [Zone chime] – the keypad can audibly signal violation of selected zones. If the zone is armed, violation will not trigger the CHIME signal.

Date/Time format – the way how date and time will be presented on the display.

LCD backlight – the way how the display backlight will work in the LCD keypad.

Keys backlight – the way how the keys backlight will work.

Auto-backlight – the way to turn on the automatic backlight of keys (in the LCD keypad, also the display).

Sounder volume – control of the volume level of sounds generated in the keypad.

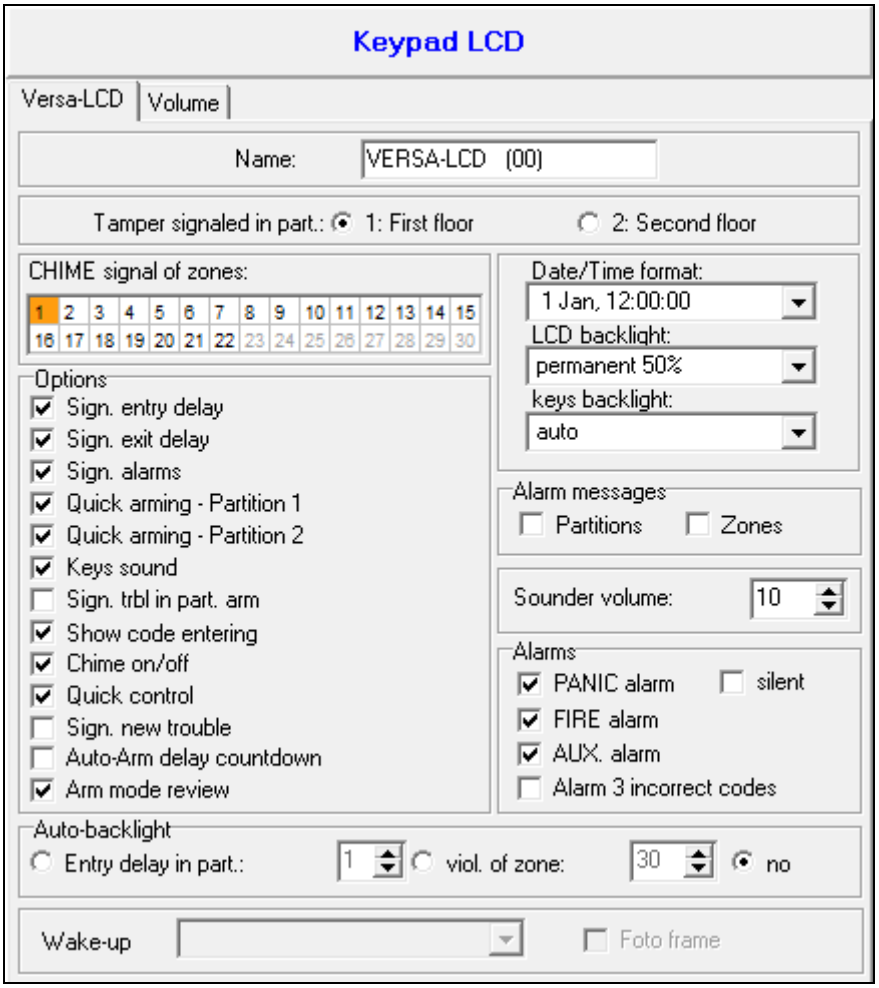


Fig. 13. DLOADX program: configuring the keypad.

Options

Sign. entry delay [Entry time sign.] – if this option is enabled, the keypad will audibly signal the entry delay countdown.

Sign. exit delay [Exit time sign.] – if this option is enabled, the keypad will audibly signal the exit delay countdown.

Sign. alarms [Alarm signalling] – if this option is enabled, the keypad will signal the alarms audibly. The alarm is signaled during the KEYPAD'S ALARM TIME (see: "Global times" p. 29).

Quick arming – Partition 1 [Part.1 QuickArm] – if this option is enabled, partition 1 can be armed without entering the code. The quick arming is not possible, if the GRADE 2 option is enabled in the control panel.

Quick arming – Partition 2 [Part.2 QuickArm] – if this option is enabled, partition 2 can be armed without entering the code. The quick arming is not possible, if the GRADE 2 option is enabled in the control panel.

Keys sound – with this option enabled, pressing the keypad keys is confirmed by beeps.

Sign. trbl in part. arm [Trbl.in part.arm] – if this option is enabled, the LED goes off after both partitions are fully armed (if the option is disabled, the LED goes off after just one of the partitions is armed in any mode).

Show code entering [Code entry ind.] – if this option is enabled, entering the code is presented:

LCD keypad – on the keypad display by asterisks,

LED keypad – by means of LEDs in the lower line of LEDs.

Chime on/off – if this option is enabled, the chime signal can be turned on/off by means of the 8tuv key (the key is to be pressed for about 3 seconds).

Quick control – if this option is enabled, the users can control the outputs by using the number keys. The 15. CONTROLLED outputs must be assigned to the keys (see: "Quick control of outputs" p. 46).

Sign. new trouble [New trbl.signal.] – if this option is enabled, the keypad will audibly signal occurrence of any new trouble (additionally, the TROUBLE MEMORY UNTIL REVIEW option must be enabled in the control panel – see: "Global options" p. 27). The signaling will be turned off after reviewing the trouble with the SYSTEM STATE user function. The new troubles will not be signaled, if the GRADE 2 option is enabled in the control panel.

Auto-Arm delay countdown [Autoarm signal.] – if this option is enabled, the auto-arm delay countdown is signaled acoustically (not applicable to the LED keypads).

Arm mode review [Arm mode check.] – if this option is enabled, holding down the ✕▼ key for about 3 seconds will display information on the partition status. The users cannot check the partition status using the ✕▼ key, if the GRADE 2 option is enabled.

Alarms

FIRE alarm – if this option is enabled, pressing the * key for approx. 3 seconds will trigger the fire alarm.

AUX. alarm [Medical alarm] – if this option is enabled, pressing the 0 key for approx. 3 seconds will trigger the auxiliary (medical) alarm.

PANIC alarm – if this option is enabled, pressing the # key for approx. 3 seconds will trigger the panic alarm.

silent [Silent panic] – if this option is enabled, the panic alarm triggered from the keypad will be a silent one, i.e. the keypad will not indicate it, there will be no audible signal, but the alarm will be reported to the monitoring station. The silent panic alarm is useful when the control panel is sending events to the monitoring station, but unauthorized persons should not be aware of the alarm being triggered.

Alarm 3 incorrect codes [3 wrong codes] – if this option is enabled, entering incorrect code three times will trigger the alarm.

Alarm messages

Partitions [Part.alarm msg.] – if this option is enabled, messages on partition alarms will be displayed (they contain the name of partition).

Zones [Zone alarm msg.] – if this option is enabled, messages on alarms from zones will be displayed (they contain the name of zone). The zone alarm messages have the priority.

The messages are presented on the display of LCD keypad.

The messages will not be displayed, if the GRADE 2 global option is enabled.

8.2.2 Volume

The volume level for different events is configurable in the case of VERSA-LCDM, VERSA-LCDR, VERSA-KWRL2 and VERSA-LCDM-WRL keypads.

Volume – volume level of the beeps generated during keypad operation (key pressing, confirmation of performed operation, etc.).

Chime – volume level of the beeps generated after zone violation (CHIME).

Entry delay – volume level of the entry delay beeps.

Exit delay – volume level of the exit delay beeps.

Fire alarm – volume level of the fire alarm beeps.

Burglary alarm – volume level when signaling burglar, panic and auxiliary (medical) alarms.

Warning alarm – volume level when signaling warning alarms.

Trouble signaling – volume level when signaling troubles.

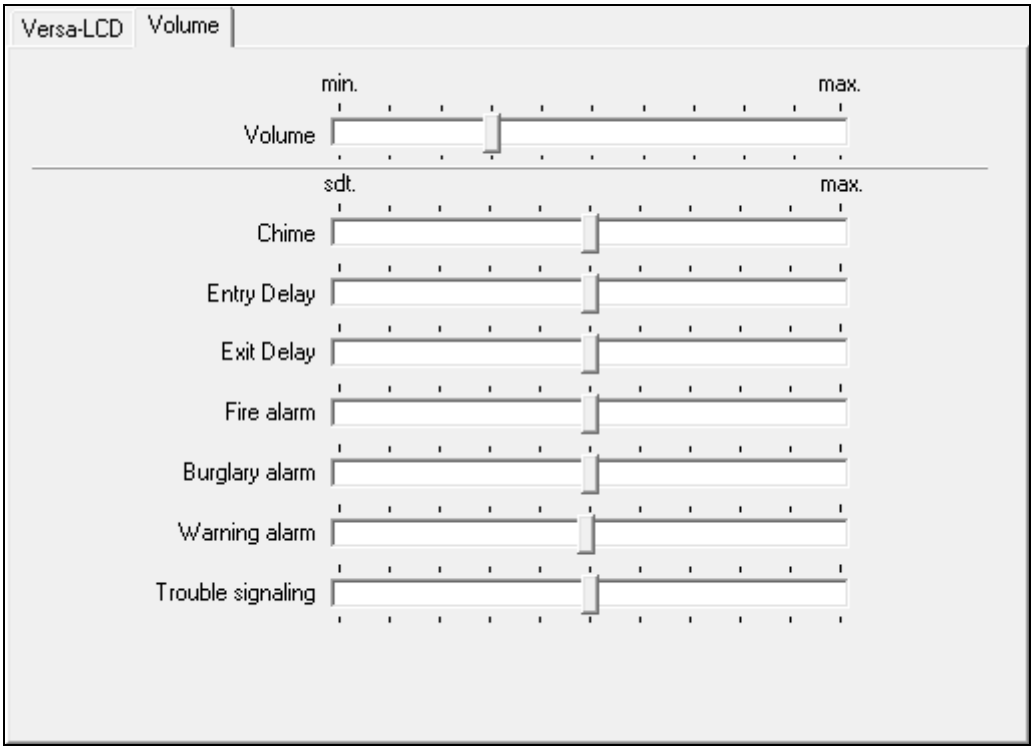


Fig. 14. DLOADX program: configuring the keypad volume.

8.2.3 Proximity cards

Parameters related to proximity card operation are available for keypads provided with proximity card readers (VERSA-LCDR, VERSA-KWRL2 and VERSA-LCDM-WRL).

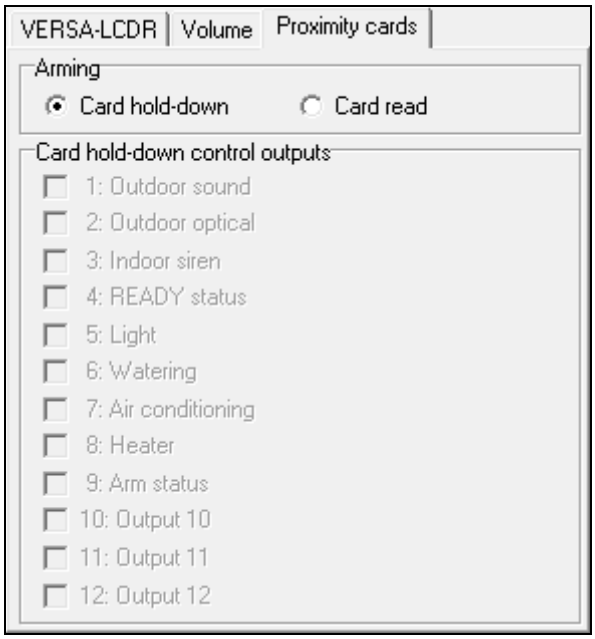


Fig. 15. DLOADX program: configuring operation with proximity cards.

Arming

Card hold-down – if you select this option, the user will have to bring the card close to the keys and hold it still for about 3 seconds to arm the system.

Card read – if you select this option, the user will only have to bring the card close to the keys to arm the system.

When configuring the keypad by using functions available in the service mode, use the PROX.CARD - ARMS option to define how to arm the system using the proximity card (option enabled = CARD READ; option disabled = CARD HOLD-DOWN).

Card hold-down control outputs

If you have selected the CARD READ option, you can permit the users to toggle the 15. CONTROLLED type outputs (the output status will change after the card is brought close to the keys and held still for about 3 seconds). Select the outputs the users will be allowed to control.

8.3 Ethernet module

The parameters and options, as described below, apply to the ETHM-1 Plus module with firmware version 2.07.

DLOADX

DLOADX->ETHM-1 connection [DLOADX→ETHM-1] – if this option is enabled, connection can be established between the DLOADX program and the alarm control panel via the module.

DLOADX server – address of the computer with DLOADX program. If the communication takes place in a wide area network, it must be a public address. You can enter either the IP address or the domain name.

Port – number of the TCP port used for communication between control panel and a computer with DLOADX program via Ethernet. You can enter values from 1 to 65535. Default value: 7090.

DLOADX key – a string of up to 12 alphanumeric characters (digits, letters and special characters) which is used for data encryption during communication with the DLOADX program via module.

SATEL service

LAN [SATEL server LAN] – if the option is enabled, the module connects to the SATEL server and the communication via the SATEL server with the control panel can be established (Connection Setup Service). This way of communication requires no additional configuring of the network device through which the module connects to the public network.

For establishing communication with the SATEL server, the DNS server must be used.

For communication via the SATEL server, the ports of 1024-65535 range are used as outgoing ports. These ports must not be blocked.

Do not report SATEL server connection trouble [No SATEL trbl.] – if this option is enabled, loss of communication with the SATEL server will not be reported.

Communication with mobile application [Mobile app.] – if this option is enabled, connection can be established between the VERSA CONTROL application and the alarm control panel via the module. The option is available if the LAN option is enabled.

Alarm 3 incorrect codes (mobile application) [Al.3 wrong codes] – if this option is enabled, entering an invalid code three times from the VERSA CONTROL application will trigger an alarm.

Push notifications – if this option is enabled, the VERSA CONTROL application can provide information about alarm system events by means of push notifications.

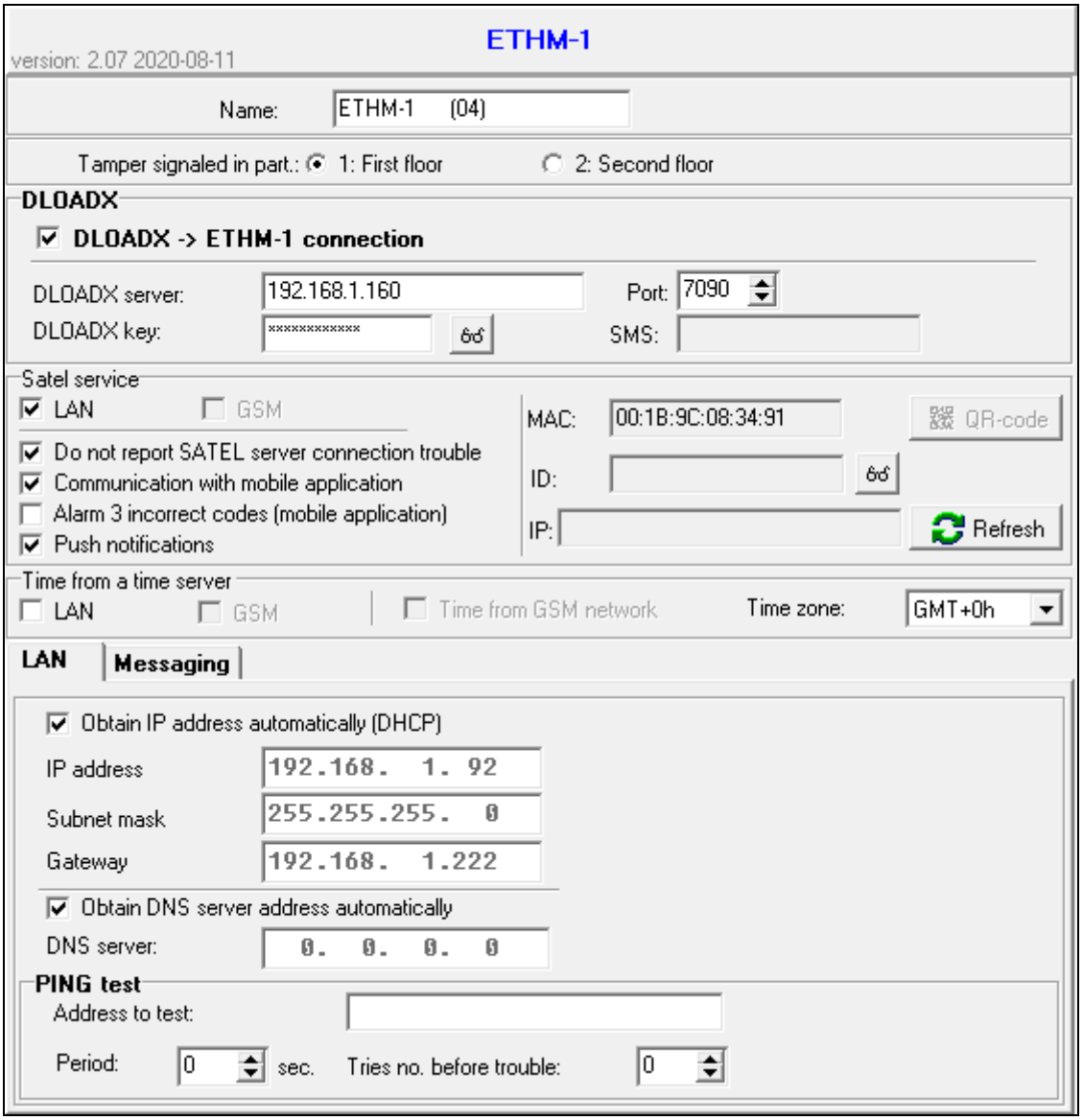


Fig. 16. DLOADX program: configuring the ETHM-1 Plus module.

Information

MAC – module hardware address.

ID – individual ID number assigned to the module by the SATEL server.

If the module is to be used in another alarm system, the hitherto used ID number must be deleted. It can be done from the keypad, when programming the Ethernet module, in the last step, if the control panel is connected to the SATEL server. Having deleted the old ID number, the module will receive a new one. The VERSA CONTROL applications using the old ID number will be unable to connect to the control panel.

IP – local address / public address of the module.

QR-code – click the button to open the window in which the QR code is displayed. The QR code contains information required when configuring settings of communication through

the SATEL server. You can read the QR code by using a mobile device or export to the file and transmit to the users. The QR code facilitates configuring the VERSA CONTROL application settings.

Refresh – click to refresh all information.

Time from a time server

LAN [Time from srvLAN] – if the option is enabled, the control panel clock will be synchronized with the time server once a day.

For communication with the time server, the DNS server must be used.

Time zone – difference between the universal time (GMT) and the zone time. The parameter is required, if the control panel clock is to be synchronized with the time server.

8.3.1 LAN

Obtain IP address automatically (DHCP) [DHCP] – if this option is enabled, the module will automatically download data on IP address, subnet mask and gateway from the DHCP server (in such a case, you do not have to program these parameters).

*The IP address assigned to the module can be read in the LCD keypad using the **MODULE VER.** user function available in the TESTS submenu. For a detailed description of the function please refer to the user manual for the control panel.*

IP address – module IP address.

Subnet mask – the mask of the subnet in which the module is working.

Gateway – IP address of the network device through which the other devices in the local network can communicate with devices in other networks.

Obtain DNS server address automatically [DHCP-DNS] – if this option is enabled, the DNS server IP address is downloaded automatically from the DHCP server. The option is available, when the OBTAIN IP ADDRESS AUTOMATICALLY (DHCP) option is enabled.

DNS server – IP address of the DNS server which is to be used by the module. It can be programmed, if the OBTAIN DNS SERVER ADDRESS AUTOMATICALLY option is disabled.

PING test

Address to test [PING] – address of the device to which a ping command to test communication is to be sent by the module. You can enter IP address or domain name.

Period [PING period] – the time interval between successive communication tests using the ping command. If value 0 is programmed, the communication test is disabled.

Tries no. before trouble [PING tries] – the number of failed communication tests (the module received no answer to the ping command sent), after which the trouble will be reported. If value 0 is programmed, the communication test is disabled.

8.4 ABAX 2 / ABAX wireless system controller

8.4.1 Parameters and options of the controller

Communication period [Polling period] – define the time intervals at which wireless devices are to communicate with the controller. Periodical communication can take place every 12, 24 or 36 seconds. During periodical communication, the devices inform the controller about their status, and the controller sends commands to the devices (switches the detectors into active/passive mode, starts/ends test mode, changes configuration of the devices, etc.). The communication period has effect on the level of energy consumption by wireless devices: the less frequent is the communication, the lower is the energy

consumption. For the battery-operated devices it means longer battery life. Moreover, when the communication takes place less frequently, more wireless devices can work within each other's operating range.

If you enable the ECO option for a wireless device (ABAX 2 controller), periodical communication between that device and the controller will take place every 3 minutes (the COMMUNICATION PERIOD parameter will have no effect on the device operation).

In the case of the AMD-103 detector and ASP-100 siren, no communication takes place during polling.

Some information and commands need to be sent immediately. Therefore, additional communication takes place when the device reports tamper, when the detector reports alarm, etc.

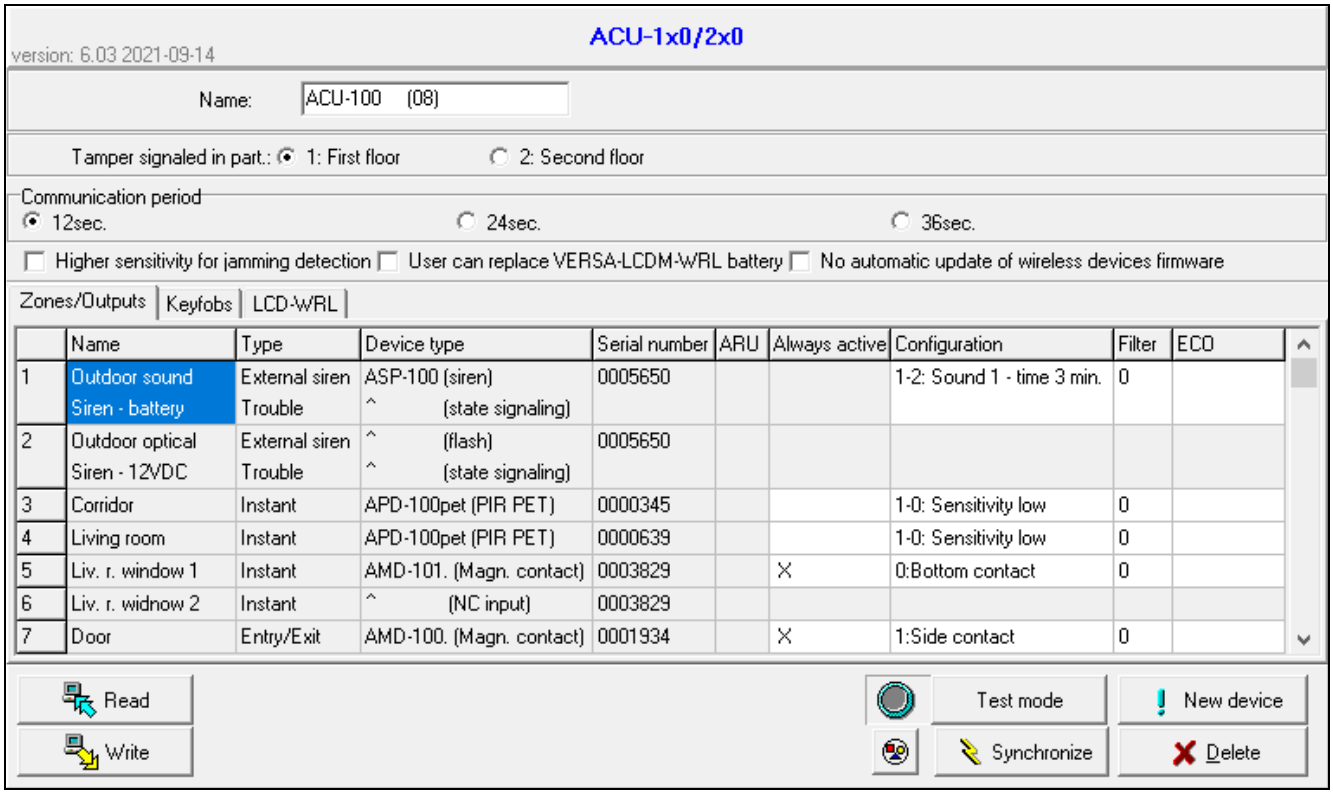


Fig. 17. DLOADX program: configuring the ABAX 2 wireless system controller and ABAX 2 wireless devices.

Higher sensitivity for jamming detection [Jam sensitivity] – if this option is enabled, the sensitivity of detection of radio communication jamming is boosted.

User can replace VERSA-LCDM-WRL battery [Usr.replaces BAT] – if this option is enabled, all users can replace battery in the VERSA-KWRL2 / VERSA-LCDM-WRL wireless keypads (for 3 minutes after the code is entered and confirmed with the * key, the status of tamper switch will not be monitored on the keypad that was used to enter the code). If the option is disabled, the battery can only be replaced by the users who have access to the REPLACE BAT. function in the 0.SERVICE submenu (the function is supported by the ABAX controller, firmware version 5.03 / ABAX 2 controller).

No automatic update of wireless devices firmware – if this option is enabled, the firmware of wireless devices registered in the controller is not updated automatically. The option is available in the ABAX 2 controller.

8.4.2 Functions

Synchronize – this function starts the procedure of synchronization, i.e. checking for presence of other ABAX wireless system controllers working within the controller operating range. The controller will synchronize the response period so that the radio transmissions of some controllers should not be mutually jammed. Synchronization is performed automatically upon starting the controller and after each operation of adding/removing devices supported by it.

The SYNCHRONIZE function does not apply to the ABAX 2 system.

Test mode – to carry out diagnostics / service work, you can start the test mode in the ABAX 2 / ABAX system. When the system is running in the test mode:

– detector LEDs are enabled,

– tamper signaling in the sirens is blocked.

The command to start/end the test mode is sent during periodical communication, i.e. with delay whose duration depends on the frequency of periodical communication. The test mode will be disabled automatically 30 minutes after:

– starting the test mode from the DLOADX program (the 30-minute period is running from the moment of exiting the controller settings),

– exiting the service mode in the control panel.

According to requirements of the EN50131 standard, the level of radio signals sent by wireless devices is reduced during the test mode operation.

For the AMD-103 detector, entering the test mode remotely is not possible.

8.4.3 Settings of ABAX 2 / ABAX system wireless devices

The wireless keypads constitute a special category of wireless devices for which a separate group of positions is reserved in the controller. For information on configuring the wireless keypads, refer to the manuals delivered with respective keypads.

Some ABAX 2 devices you can only configure by using the DLOADX program (e.g. ACD-220 and ADD-200 detectors).

Always active [Active mode] – the option is available for the most of wireless detectors. If enabled, the detector is permanently switched over to the active mode (see “ABAX 2 / ABAX wireless detectors” p. 63).

The AMD-103 detector and the wireless detectors assigned to 24-h zones are always in the active mode, therefore the ALWAYS ACTIVE option does not have to be enabled for them.

The battery life time in the detectors switched permanently into the active mode is shorter than in those which are periodically switched to the passive mode.

Configuration – for some devices you can configure additional parameters and options. Shown in parentheses is the device name in the ABAX 2 system (if the device is identified in the alarm system by the name known from the ABAX system). Shown in square brackets is information about the number of zone for which additional parameters are to be programmed if the device takes up more than one zone.

ACD-220 – wireless curtain detector. You can configure sensitivity.

ADD-200 – wireless outdoor dusk and temperature detector. You can configure:

- sensitivity of the dusk sensor (detection threshold) [first zone],

- temperature threshold parameters [second zone]:
  - threshold type: high (when the temperature rises above the defined value, alarm will be triggered) or low (when the temperature drops below the defined value, alarm will be triggered),
  - temperature,
  - tolerance.

AGD-100 (AGD-200) – wireless glass-break detector. You can configure sensitivity.

AMD-100 (AMD-200) / **AMD-101 (AMD-201)** – wireless magnetic contact. You can select the active reed switch (not applicable to the AMD-200 / AMD-201 detector, which does not have two reed switches).

AMD-102 (AMD-202) – wireless magnetic contact with input for roller shutter detector. You can:

- select the active reed switch of magnetic contact (not applicable to the AMD-202 detector, which does not have two reed switches) [first zone].
- configure parameters of roller shutter input [second zone]:
  - number of pulses after which the roller shutter input will trigger alarm,
  - time period during which the defined number pulses must occur for the roller shutter input to trigger alarm.

AOCD-250 (AOCD-260) – wireless outdoor dual technology curtain detector. You can configure:

- sensitivity of the PIR sensor,
- sensitivity of the microwave sensor.

AOD-200 (AOD-210) – wireless outdoor dual technology motion detector. You can configure:

- sensitivity of the PIR sensor,
- sensitivity of the microwave sensor,
- sensitivity of the dusk sensor (detection threshold).

APD-100 (APD-200) – wireless passive infrared detector. You can configure sensitivity.

APD-100 (APD-200 Pet) – wireless passive infrared detector with pet immunity. You can configure:

- sensitivity,
- pet immunity option (not applicable to the APD-200 Pet detector, which is immune to pet movement at all times).

APMD-150 (APMD-250) – wireless dual technology detector. You can configure:

- sensitivity of the PIR sensor,
- sensitivity of the microwave sensor,
- manner of operation in the test mode.

ARD-100 (ARD-200) – wireless reorientation detector. You can configure sensitivity.

ASD-150 (ASD-250) – wireless smoke detector. You can configure:

- option to indicate alarm from other ASD-250 / ASD-150 detectors,
- option to send alarm to other ASD-250 / ASD-150 detectors.

AVD-100 (AVD-200) – wireless shock detector and magnetic contact. You can:

- select the active reed switch of magnetic contact (not applicable to the AVD-200 detector, which does not have two reed switches) [first zone],
- configure the shock detector parameters [second zone]:
  - sensitivity (registering a shock meeting the sensitivity criterion will trigger alarm),

– number of shocks, registering of which by the detector will trigger an alarm – the shocks do not have to meet the sensitivity criterion (not applicable to the AVD-200 detector, which does not count the shocks).

Working parameters of the shock detector are independently analyzed. The detector will report an alarm after a single strong shock caused by a heavy impact, as well as after a series of weak shocks caused by a series of slight impacts.

ASP-100 (ASP-200) – wireless outdoor siren. You can configure:

- type of acoustic signaling;
- maximum duration of signaling.

ASP-105 – wirelessly triggered outdoor siren. You can configure:

- type of acoustic signaling,
- maximum duration of acoustic signaling.

ASP-205 (ASP-215) – wireless indoor siren. You can configure the signaling parameters for both positions occupied by the siren (which enables two different types of signaling to be programmed):

- maximum duration of signaling (optical and acoustic),
- type of acoustic signaling,
- optical signaling option.

ASW-100 (ASW-200) – smart plug. You can select operating mode.

Filter – the number of consecutive communication periods without connection between the device and the controller after which loss of communication with the device will be reported. You can enter values from 0 to 50. Entering 0 disables the check for device presence in the system.

In the case of the AMD-103 magnetic contact and ASP-100 siren, the presence check is performed in a different way than for the other ABAX 2 / ABAX system devices. If the value programmed for the FILTER parameter differs from 0, the lack of presence will be reported if no transmission from the AMD-103 magnetic contact / ASP-100 siren is received within one hour.

ECO – if this option is enabled, periodical communication with the device takes place every 3 minutes. Thus the battery life can be extended up to four times. The option is available in the ABAX 2 controller.

Remember that with the ECO option enabled for:

detectors – delay between arming / disarming and changing the detector operating mode (active / passive) can be up to three minutes,

ASP-215 siren – delay in starting / stopping the signaling can be up to three minutes.

8.4.4 Configuring the ABAX 2 / ABAX wireless devices

DLOADX program

You can configure the wireless devices as follows: “VERSA – Structure” window →“Hardware” tab →“Expansion modules” branch →*[ABAX 2 / ABAX controller name]* →“Zones/Outputs” tab. Before making any changes, click on the “Read” button, and after making the changes – on the “Write” button (the data relating to the wireless devices are not read after clicking on the  button or saved after clicking on the  button in the DLOADX program main menu). Described below is how the additional parameters and options should be programmed in the “Configuration” column.

ACD-220

Enter a digit from the 1 to 3 range to set the sensitivity (1 – low, 2 – medium, 3 – high).

ADD-200

Dusk sensor – enter a number from the 1 to 16 range to determine sensitivity (1 – minimum; 16 – maximum).

Temperature sensor – enter in turn:

- letter H (high temperature threshold) or L (low temperature threshold),
- number from a range of -30 to +70 (with 0.5 accuracy) to define temperature,
- number from a range of 0.5 to 10 (with 0.5 accuracy) to define tolerance.

AGD-100 (AGD-200)

Enter a digit from the 1 to 3 range to set the sensitivity (1 – low, 2 – medium, 3 – high).

AMD-100 (AMD-200) / AMD-101 (AMD-201)

Enter the digit 0 (bottom reed switch) or 1 (side reed switch) to determine which of the two reed switches is to be active. In the case of the AMD-200 and AMD-201 detectors – do not configure.

AMD-102 (AMD-202)

Magnetic contact – enter the digit 0 (bottom reed switch) or 1 (side reed switch) to determine which of the two reed switches is to be active. In the case of the AMD-202 detector – do not configure.

Roller shutter input – enter 2 digits:

1st digit – number of pulses: from 1 to 8.

2nd digit – pulse validity: 0 (30 seconds), 1 (120 seconds), 2 (240 seconds) or 3 (unlimited duration).

AOCD-250 (AOCD-260)

Enter 2 digits:

1st digit – sensitivity of PIR sensor: from 1 to 4 (1 – minimum; 4 – maximum).

2nd digit – sensitivity of microwave sensor: from 1 to 8 (1 – minimum; 8 – maximum).

AOD-200 (AOD-210)

Enter 3 digits:

1st digit – sensitivity of PIR sensor: from 1 to 4 (1 – minimum; 4 – maximum).

2nd digit – sensitivity of microwave sensor: from 1 to 8 (1 – minimum; 8 – maximum).

3rd digit – sensitivity of dusk sensor: from 1 to 4 (1 – minimum; 4 – maximum).

APD-100 (APD-200)

Enter a digit from the 1 to 3 range to set the sensitivity (1 – low, 2 – medium, 3 - high).

APD-100 (APD-200 Pet)

Enter 2 digits:

1st digit – sensitivity: 1 (low), 2 (medium) or 3 (high),

2nd digit – pet immunity option: 0 (disabled) or 1 (enabled). In the case of the APD-200 Pet detector – do not configure.

APMD-150 (APMD-250)

Enter 3 digits:

1st digit – sensitivity of PIR sensor: from 1 to 4 (1 – minimum; 4 – maximum).

2nd digit – sensitivity of microwave sensor: from 1 to 8 (1 – minimum; 8 – maximum).

3rd digit – the way of operation in the test mode: 0 (alarm triggered after motion is sensed by both detectors), 1 (alarm triggered after motion is sensed by infrared detector) or 2 (alarm triggered after motion is sensed by microwave detector).

ARD-100 (ARD-200)

Enter a number from the 1 to 16 range to determine sensitivity (1 – minimum; 16 - maximum).

ASD-150 (ASD-250)

Enter 2 digits:

1st digit – option to signal alarm from other ASD-150 / ASD-250 detectors: 0 (disabled) or 1 (enabled).

2nd digit – option to send out alarm to other ASD-150 / ASD-250 detectors: 0 (disabled) or 1 (enabled).

AVD-100 (AVD-200)

Magnetic contact – enter the digit 0 (bottom reed switch) or 1 (side reed switch) to determine which of the two reed switches is to be active. In the case of the AVD-200 detector – do not configure.

Shock detector – enter 2 digits:

1st digit – sensitivity: from 1 to 8 (1 – minimum; 8 – maximum).

2nd digit – number of shocks: from 0 to 7. For the value 0, shocks are not counted. In the case of the AVD-200 detector – do not configure.

ASP-100 (ASP-200)

Enter 2 digits:

1st digit – type of acoustic signaling: from 1 to 4.

2nd digit – maximum duration of signaling: 1 (1 minute), 2 (3 minutes), 3 (6 minutes) or 4 (9 minutes).

ASP-105

Enter 2 digits:

1st digit – type of acoustic signaling: from 1 to 4.

2nd digit – maximum duration of acoustic signaling: 1 (1 minute), 2 (3 minutes), 3 (6 minutes) or 4 (9 minutes).

ASP-205 (ASP-215)

For each position taken on the list by the siren, enter 3 digits:

1st digit – maximum duration of signaling: 1 (1 minute), 2 (3 minutes), 3 (6 minutes) or 4 (9 minutes).

2nd digit – type of acoustic signaling: 0 (disabled), 1 (sound type 1), 2 (sound type 2) or 3 (sound type 3).

3rd digit – optical signaling: 0 (disabled) or 1 (enabled).

ASW-100 (ASW-200)

Enter 0 (only remote control), 1 (remote or manual control) or 2 (remote or manual control, but with option to manually block the remote control).

LCD keypad

You can configure the settings of wireless device:

- immediately after adding the device to the system (for the procedure of adding ABAX 2 / ABAX wireless devices, refer to the INSTALLER MANUAL),
- using the CONFIG.DEVICE function (SERVICE MODE ▶2. HARDWARE ▶1. KPDS & EXPS ▶3. WIRELESS DEV. ▶2. CONFIG.DEVICE). Having started the function, use the [▲] and [▼] keys to select the zone to which the wireless device is assigned and press [#].

The programming is performed using the “step by step” method (see: p. 6). Described below is how to configure the devices for which additional settings are available.

AGD-100 (AGD-200)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
2. Press any numeric key to define whether the detector is to be always active (· – no, ▮ - yes), and then press [#].
3. Enter a digit from the 1 to 3 range to define sensitivity (1 – low, 2 – medium, 3 – high), and then press [#].

AMD-100 (AMD-200) / AMD-101 (AMD-201)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
2. Press any numeric key to define whether the detector is to be always active (· – no, ▮ - yes), and then press [#].
3. Depending on the detector:
   – AMD-100 / AMD-101 – use the [▲] and [▼] keys to select which of the two reed switches (bottom or side) of the magnetic contact is to be active, and then press [#],
   – AMD-200 / AMD-201 – press [#] (the setting is irrelevant).

AMD-102 (AMD-202)

For the magnetic contact:

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
2. Press any numeric key to define whether the detector is to be always active (· – no, ▮ - yes), and then press [#].
3. Depending on the detector:
   – AMD-102 – use the [▲] and [▼] keys to select which of the two reed switches (bottom or side) of the magnetic contact is to be active, and then press [#],
   – AMD-202 – press [#] (the setting is irrelevant).

For the roller shutter input:

1. Enter a digit from the 1 to 8 range to define the number of pulses that will trigger alarm, and then press [#].
2. Use the [▲] and [▼] keys to select the pulse validity time (30, 120 or 240 seconds or unlimited time), and then press [#].

AOCD-250 (AOCD-260)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].

2. Press any numeric key to define whether the detector is to be always active (· – no, 1 - yes), and then press #.
3. Enter a digit from the 1 to 4 range to define sensitivity of the PIR sensor (1 – minimum; 4 – maximum), and then press #.
4. Enter a digit from the 1 to 8 range to define sensitivity of the microwave sensor (1 - minimum; 8 – maximum), and then press #.

AOD-200 (AOD-210)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press #.
2. Press any numeric key to define whether the detector is to be always active (· – no, 1 - yes), and then press #.
3. Enter a digit from the 1 to 4 range to define sensitivity of the PIR sensor (1 – minimum; 4 – maximum), and then press #.
4. Enter a digit from the 1 to 8 range to define sensitivity of the microwave sensor (1 - minimum; 8 – maximum), and then press #.
5. Enter a digit from the 1 to 4 range to define sensitivity of the dusk sensor (1 – minimum; 4 – maximum), and then press #.

APD-100 (APD-200)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press #.
2. Press any number key to define whether the detector is to be always active (· – no, 1 - yes), and then press #.
3. Enter a digit from the 1 to 3 range to define sensitivity (1 – low, 2 – medium, 3 – high), and then press #.

APD-100 (APD-200 Pet)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press #.
2. Press any number key to define whether the detector is to be always active (· – no, 1 - yes), and then press #.
3. Enter a digit from the 1 to 3 range to define sensitivity (1 – low, 2 – medium, 3 – high), and then press #.
4. Depending on the detector:
   – APD-100 – press any number key to define whether the pet immunity option is to be enabled (· – no, 1 – yes), and then press #,
   – APD-200 Pet – press # (the setting is irrelevant).

APMD-150 (APMD-250)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press #.
2. Press any numeric key to define whether the detector is to be always active (· – no, 1 - yes), and then press #.
3. Enter a digit from the 1 to 4 range to define sensitivity of the PIR sensor (1 – minimum; 4 – maximum), and then press #.
4. Enter a digit from the 1 to 8 range to define sensitivity of the microwave sensor (1 - minimum; 8 – maximum), and then press #.

5. Use the [▲] and [▼] keys to select how the detector will work in the test mode (PIR+MW, PIR or MW), and then press [#].

ARD-100 (ARD-200)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
2. Press any numeric key to define whether the detector is to be always active (· – no, ■ - yes), and then press [#].
3. Enter a number from the 1 to 16 range to define sensitivity (1 – minimum; 16 – maximum), and then press [#].

ASD-150 (ASD-250)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
2. Press any numeric key to define whether the detector is to signal alarm from other ASD-150 / ASD-250 detectors (· – no, ■ – yes), and then press [▼].
3. Press any numeric key to define whether the detector is to send out alarm to other ASD-150 / ASD-250 detectors (· – no, ■ – yes), and then press [#].

AVD-100 (AVD-200)

For the magnetic contact:

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
2. Press any numeric key to define whether the detector is to be always active (· – no, ■ - yes), and then press [#].
3. Depending on the detector:
   – AVD-100 – use the [▲] and [▼] keys to select which of the two reed switches (bottom or side) of the magnetic contact is to be active, and then press [#].
   – AVD-200 – press [#] (the setting is irrelevant).

For the shock detector:

1. Enter a digit from the 1 to 8 range to define sensitivity of the vibration detector (1 - minimum; 8 – maximum), and then press [#].
2. Depending on the detector:
   – AVD-100 – enter a digit from the 0 to 7 range to define the number of shocks that will trigger alarm, and then press [#],
   – AVD-200 – press [#] (the setting is irrelevant).

ASP-100 (ASP-200)

1. Enter 0, if presence of the siren is not to be checked, or enter a number from the 1 to 50 range, if presence of the siren is to be checked (the number entered is irrelevant – if there is no communication during a 1-hour period, absence of the device will be reported), and then press [#].
2. Use the [▲] and [▼] keys to select the type of acoustic signaling, and then press [#].
3. Use the [▲] and [▼] keys to define the maximum duration of signaling, and then press [#].

ASP-105

4. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
5. Use the [▲] and [▼] keys to select the type of acoustic signaling, and then press [#].
6. Use the [▲] and [▼] keys to define the maximum duration of acoustic signaling, and then press [#].

ASP-205 (ASP-215)

You can program two different ways of signaling:

- having selected the first of the zones to which the siren is assigned: signaling triggered by the first output controlling the siren,
- having selected the second of the zones to which the siren is assigned: signaling triggered by the second output controlling the siren.

Configuration is similar for both zones, however, the step in which the rules of device presence control are defined is skipped for the second zone.

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
2. Use the [▲] and [▼] keys to define how the acoustic signaling will work (· - disabled; 1, 2 or 3 – type of acoustic signaling), and then press [#].
3. Use the [▲] and [▼] keys to define the maximum duration of signaling, and then press [#].
4. Define whether the optical signaling is to be enabled (· – no, ■ – yes), and then press [#].

ASW-100 (ASW-200)

1. Enter a number from the 0 to 50 range to define the rules of device presence control, and then press [#].
2. Use the [▲] and [▼] keys to define the way of control (“inactive” – only remote control; “interim control” – remote or manual control; “combined control” – remote or manual control, but with option to manually block the remote control), and then press [#].

8.4.5 Specific character of the operation of ABAX 2 / ABAX wireless devices

When configuring the alarm system zones and outputs to which the wireless devices are assigned, you must take into account the specific character of operation of individual devices.

ABAX 2 / ABAX wireless detectors

The zone to which a wireless detector is assigned is activated when the detector reports alarm (select the appropriate zone type). If a detector tamper is to trigger the tamper alarm, program the zone as 2EOL/NC or 2EOL/NO.

Operation of the detector is affected by the state of partition to which the zone belongs:

partition disarmed – the detector operates in **passive mode**. This operating mode prolongs the battery life. Detector informs the controller about its status during periodical communication (only the tamper information is sent immediately).

partition armed – the detector operates in **active mode**. Detector informs the controller about alarm or tamper immediately.

Switching the detector from passive mode to active and vice versa takes place during periodical communication. It results in a delay whose duration depends on the frequency of periodical communication (with the ECO option enabled, delay can be up to 3 minutes).

The AMD-103 detector and the wireless detectors assigned to 24-h zones, i.e. always armed, are in active mode at all times. For most detectors, you can enable the ALWAYS ACTIVE option (see: “Settings of ABAX 2 / ABAX system wireless devices” p. 55).

According to the EN50131-3 standard all ABAX 2 / ABAX Hold-Up devices must be always in active mode.

The battery life time in the detectors switched permanently into the active mode is shorter than in those which are periodically switched to the passive mode. However, if the specific character of a detector or its installation place is such that the number of alarms is low, switching the detector permanently into the active mode will not have a significant effect on the battery life.

ABAX 2 / ABAX wireless sirens

Turning on the output to which the wireless siren is assigned will trigger the signaling. Depending on the siren:

ASP-100 / **ASP-200** – the first output controls the acoustic signaling, the second – the optical signaling. Thanks to a high-capacity battery, the siren can receive transmissions from the controller at any time. Therefore, the commands to start/stop signaling are sent to the siren immediately.

ASP-105 – the first output controls the acoustic signaling, the second – the optical signaling. The method of powering the siren enables it to receive transmissions from the controller at any time. Therefore, the commands to start/stop signaling are sent to the siren immediately.

ASP-205 / **ASP-215** – both outputs can control the acoustic and optical signaling. This enables two different, independently triggered types of signaling to be configured. The outputs can control separately the acoustic and optical signaling or trigger other signaling for different alarms (e.g. burglary and fire). Given its low-capacity battery, the siren can receive transmissions from the controller during periodical communication only. Therefore, the commands to start/stop signaling are sent to the siren during periodical communication. Consequently, the operating time of outputs controlling the siren should be longer than the communication period.

The signaling will stop after the maximum signaling time expires, even if the output is still active (the exception is the optical signaling in the ASP-105 siren, which is active as long as the output is active).

The zones to which the wireless siren is assigned are activated in the following cases (select the appropriate zone type):

ASP-100 / **ASP-200** – first zone: low battery; second zone: tamper.

ASP-105 – first zone: low battery; second zone: 12 VDC power loss.

ASP-205 – both zones: low battery.

ASP-215 – both zones: starting the signaling.

If the siren tamper is to trigger tamper alarm, program the zone as 2EOL/NC or 2EOL/NO.

The tamper information is sent immediately, while the trouble information:

ASP-100 – during periodical transmission, which is sent every 15 minutes,

ASP-105 / **ASP-200** / **ASP-205** / **ASP-215** – during periodical communication.

Tamper alarm on opening the tamper switch in the siren:

ASP-100 / **ASP-200** – lasts for the maximum duration of signaling programmed for the siren (sound type selected during programming and optical signaling);

ASP-105 – lasts for the maximum duration of acoustic signaling programmed for the siren (sound type selected during programming and optical signaling);

ASP-205 / **ASP-215** – lasts 3 minutes (sound type 1 and optical signaling).

Tamper signaling is blocked:

- *when the control panel is running in service mode,*
- *when the ABAX 2 / ABAX system is running in test mode (ASP-105 / ASP-200 / ASP-205 / ASP-215),*
- *for 10 minutes after connecting the battery (ASP-100 / ASP-200),*
- *for 40 seconds after power-on (ASP-105) / installing the battery (ASP-205 / ASP-215).*

It enables installation work to be carried out. Opening the tamper switch will not trigger loud signaling, but information on tamper will be sent (when in service mode, the control panel will not signal the tamper alarms). The command to block/unblock the signaling connected with starting / ending the test mode or the service mode is sent during the response time.

Wireless expanders of hardwired zones and outputs

The wireless expander of hardwired zones and outputs (ACX-200 / ACX-201 / ACX-210 / ACX-220) takes up 4 zones and 4 outputs in the system. You can configure the alarm system zone/output to which expander zone/output is assigned in much the same way as hardwired zones/outputs. You must, however, keep in mind that sensitivity of the expander zones may be different from that programmed in the control panel:

- from 20 ms to 140 ms – the same as the value programmed in the control panel,
- above 140 ms – only some values are available: 400 ms, 500 ms, 700 ms, etc. every 200 ms (the programmed value is rounded up to that supported by the expander).

The EN50131-3 standard requires that zones must react to signals lasting more than 400 ms. Therefore, select 400 ms when programming sensitivity of the alarm zones.

Information on the state of zones and commands to change the state of outputs are sent immediately. Zone settings are sent during periodical communication.

If communication with the controller is lost, all previously activated outputs will be deactivated after 20 response periods.

Additionally, the ACX-201 expander module sends information about:

- status of AUX1 and AUX2 power supply outputs – information on overload is sent when the AUX1 or AUX2 output load exceeds 0.5 A.
- battery status – information on low battery is sent when the battery voltage drops below 11 V for more than 12 minutes (3 battery tests). The expander will kept sending this information to the controller until the battery voltage rises and remains above 11 V for longer than 12 minutes (3 battery tests).
- AC power status – information on the loss of power supply is sent when the AC power loss lasts for more than 30 seconds. The AC power restore is reported with the same delay.

Low battery information for the first zone of ACX-201 expander indicates overload of the AUX1 or AUX2 power supply output, for the second zone – discharged battery, for the third zone – loss of AC power.

If the ACX-220 expander is powered from a power supply unit connected to the APS connector, the low battery information provided by the control panel means:

first zone – power supply overload,

second zone – low battery,

third zone – AC mains loss.

Smart plug / 230 VAC wireless controllers

Turning on the output to which the plug / controller is assigned turns on the relay controlling the 230 VAC circuit (turns on the device connected to the plug / controller).

The zone to which the plug / controller is assigned is activated when:

- operating modes 1 and 2: the relay controlling the 230 VAC circuit is turned on,
- operating mode 0: the plug button is pressed / the controller input is activated.

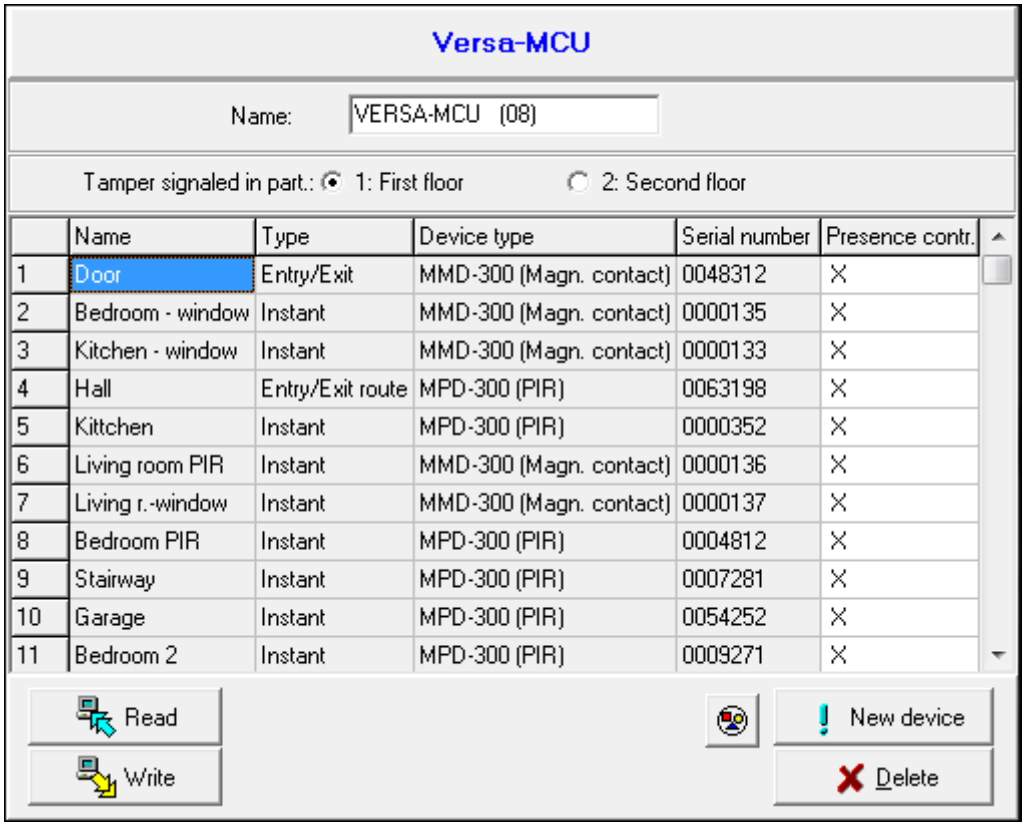
Select the appropriate zone type.

8.5 MICRA wireless system controller

The MRU-300 repeater is identified as the MMD-300 detector. When configuring it, proceed in the same way as with a detector.

8.5.1 Presence control of MICRA (433 MHz) wireless detectors

Presence contr. [Presence control] – if this option is enabled, the detector is checked for presence. If no transmission is received from the detector within an hour, trouble will be reported (loss of communication with the detector).



	Name	Type	Device type	Serial number	Presence contr.
1	Door	Entry/Exit	MMD-300 (Magn. contact)	0048312	X
2	Bedroom - window	Instant	MMD-300 (Magn. contact)	0000135	X
3	Kitchen - window	Instant	MMD-300 (Magn. contact)	0000133	X
4	Hall	Entry/Exit route	MPD-300 (PIR)	0063198	X
5	Kittchen	Instant	MPD-300 (PIR)	0000352	X
6	Living room PIR	Instant	MMD-300 (Magn. contact)	0000136	X
7	Living r.-window	Instant	MMD-300 (Magn. contact)	0000137	X
8	Bedroom PIR	Instant	MPD-300 (PIR)	0004812	X
9	Stairway	Instant	MPD-300 (PIR)	0007281	X
10	Garage	Instant	MPD-300 (PIR)	0054252	X
11	Bedroom 2	Instant	MPD-300 (PIR)	0009271	X

Fig. 18. DLOADX program: configuring the MICRA wireless system controller and MICRA (433 MHz) wireless detectors.

8.5.2 Configuring the MICRA (433 MHz) wireless detectors

DLOADX program

You can enable/disable the presence control option: "VERSA – Structure" window →"Hardware" tab →"Expansion modules" branch →*[VERSA-MCU controller name]*. Before making any changes, click on the "Read" button, and after making the changes – on the "Write" button (the data relating to the MICRA (433 MHz) wireless detectors are not read after clicking on the  button or saved after clicking on the  button in the DLOADX program main menu). To enable / disable the option, click on the "Presence contr." column (symbol X indicates that the option is enabled).

LCD keypad

You can enable/disable the presence control option:

- immediately after adding a detector to the system (for the procedure of adding MICRA (433 MHz) wireless detectors, refer to the INSTALLER MANUAL),
- using the CONFIG.DEVICE function (SERVICE MODE ▶2. HARDWARE ▶1. KPDS & EXPS ▶3. WIRELESS DEV. ▶2. CONFIG.DEVICE). Having started the function, use the [▲] and [▼] keys to select the zone to which the wireless detector is assigned and press [#].

To enable/disable the option, press any numeric key (· – option disabled, ▮ – option enabled), and then press [#].

8.5.3 MICRA (433 MHz) wireless detectors and zone programming

The zone to which a wireless detector is assigned is activated when the detector reports alarm (select the appropriate zone type). If a detector tamper is to trigger the tamper alarm, program the zone as 2EOL/NC or 2EOL/NO.

The detector operating mode affects the way the zone works:

Normal – the detector reports each alarm. If the detector also reports the alarm restore (e.g. magnetic contact or water flood detector), the zone status corresponds to the detector status. If the detector does not report the alarm restore (e.g. motion detector or glass-break detector), the zone is active for 2 seconds after receiving information on the alarm.

Energy save (available in some detectors) – the detector reports alarms not more often than every 3 minutes (the next alarms triggered within 3 minutes from sending the information about the alarm will not result in a radio transmission). The zone is active for 2 seconds after receiving information on the alarm.

The operating mode does not affect the tamper notification. The information on tamper is sent always.

8.6 Proximity card arm/disarm device

Partition list

R [LED R – part.1 / LED R – part.2] – the function to be run in the partition, if the card is moved away from the device when the red LED is ON:

[Full arm] – full arming,

blank field [Does not arm] – none.

G [LED G – part.1 / LED G – part.2] – the function to be run in the partition, if the card is moved away from the device when the green LED is ON (mode A):

[Full arm] – full arming,

[Stay night arm] – night arming,

[Stay day arm] – day arming,

[Disarm] – disarming,

blank field [Does not arm] – none.

Y [LED Y – part.1 / LED Y – part.2] – the function to be run in the partition, if the card is moved away from the device when the yellow LED is ON (mode B):

[Full arm] – full arming,

[Stay night arm] – night arming,

[Stay day arm] – day arming,

[Disarm] – disarming,

blank field [Does not arm] – none.

In the DLOADX program, to define reaction of the partition after moving the card away from the module, double click on the field corresponding to the selected partition. The icon displayed in the field will change accordingly. In the LCD keypad, select the partition response from the list.

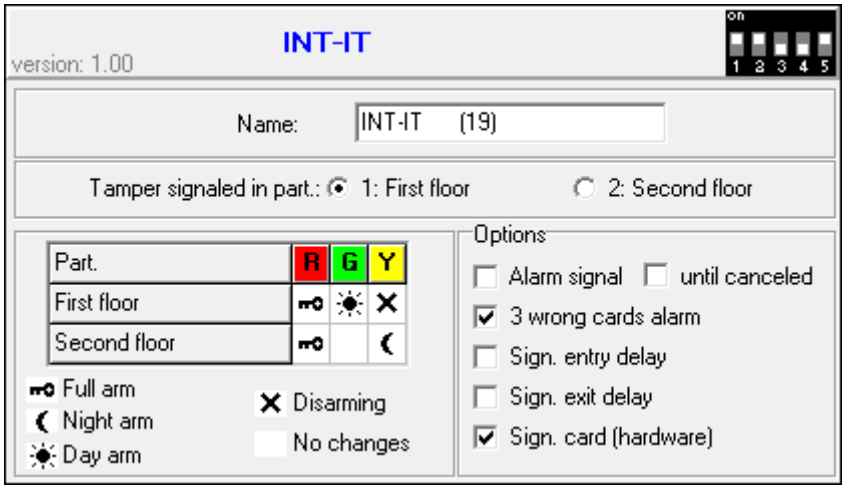


Fig. 19. DLOADX program: configuring the proximity card arm/disarm device.

Options

Alarm signal [Timed alarm sign] – if the option is enabled, the device is audibly signaling alarms during the KEYPAD'S ALARM TIME.

until canceled [Alm.until clear] – if the option is enabled, the device is audibly signaling alarms until they are cleared.

3 wrong cards alarm [3 wrng cards al.] – if the option is enabled, using an unknown card three times will trigger an alarm.

Sign. entry delay [Entry delay sig.] – if the option is enabled, the device is audibly signaling the entry delay countdown.

Sign. exit delay [Exit delay sign.] – if the option is enabled, the device is audibly signaling the exit delay and auto-arm delay countdown.

Sign. card (hardware) [Hardware signal.] – if the option is enabled, the device is signaling by a single beep that the card code has been read out or the LED has lit up (the code is sent to the control panel after removal of the card and only then the device is audibly signaling its reaction to the read code).

9. Timers

The timer compares the time to that of the control panel clock and executes the selected function at the programmed time. Using the timers, it is possible to control the armed mode of partitions and the outputs 15. CONTROLLED. You can program 4 timers.

9.1 Programming the timers

You can program timers:

- DLOADX program: "VERSA – Timers" window (Fig. 20).

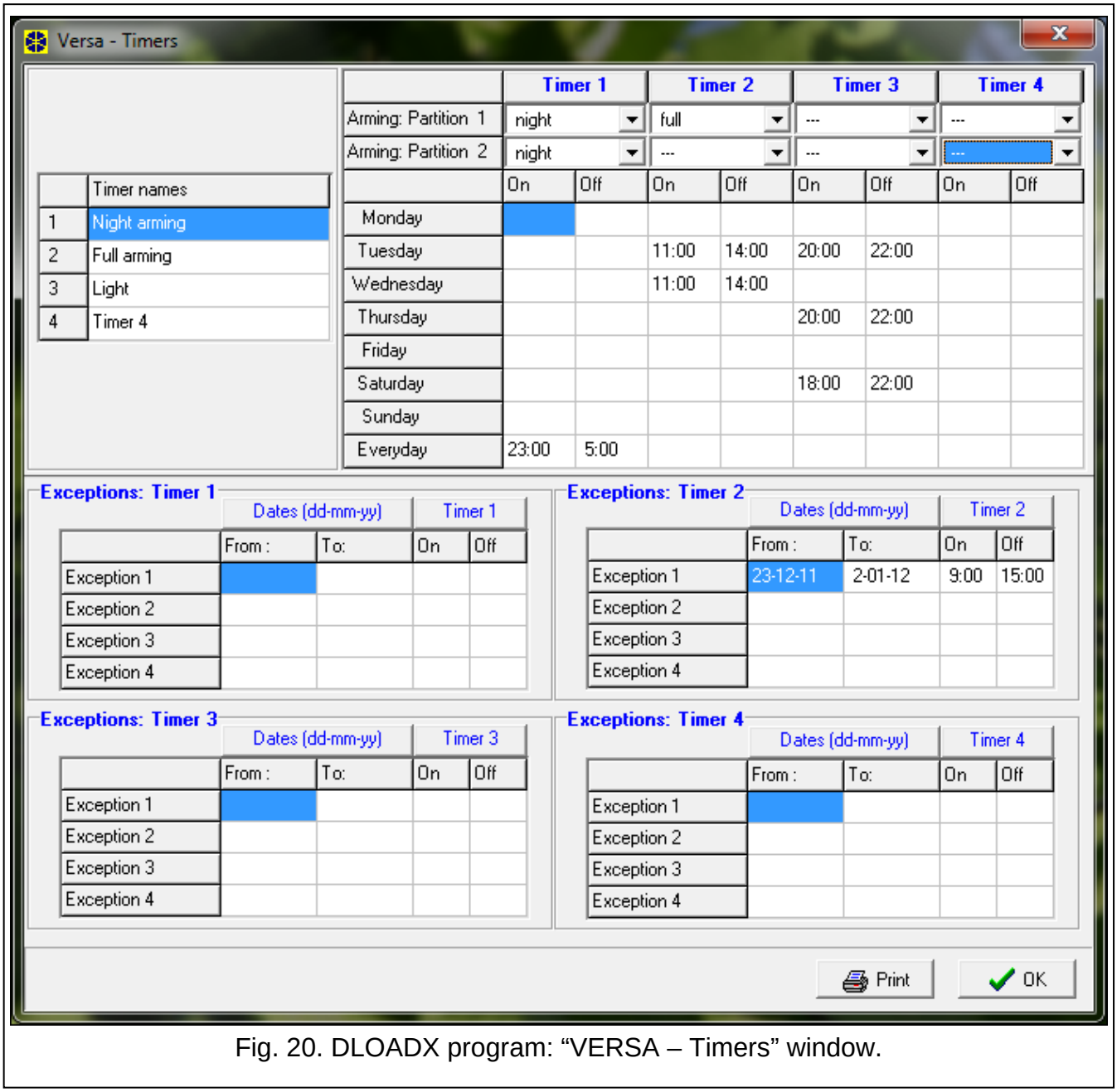


Fig. 20. DLOADX program: "VERSA – Timers" window.

- keypad:
  - functions available in the service menu, TIMERS submenu, enable programming of the timer names by means of LCD keypad (SERVICE MODE ▶4. TIMERS),
  - the TIMERS function available in the user menu enables programming of the other timer parameters ([code] ✱ ▶6. SETTINGS ▶3. TIMERS). The programming is performed using the "step by step" method (see: p. 6).

9.2 Timer parameters

Name – individual timer name (up to 16 characters).

Weekly schedule – the time of starting/ending timer for each day of the week and everyday (the timer can be started/ended twice a day: according to the settings scheduled for the given day of the week and according to the everyday settings).

Exception – the period during which the timer will be started/ended at a different time than indicated in the weekly schedule. 4 exceptions can be programmed for a timer. You can program for each exception:

- the date from which the exception will apply,
- the date to which the exception will apply,
- the timer start/end time when an exception applies.

Partition arming mode – the arming mode that will be activated in the partition when the timer will start.

10. Reporting

The control panel can send event codes to the monitoring station by using the following transmission paths:

- analog telephone line [built-in analog telephone communicator],
- Ethernet network [requires the ETHM-1 / ETHM-1 Plus module to be connected].

If both transmission paths are used, the control panel will first try to send the event code through the Ethernet network, and only when the attempt fails, it will switch over to the telephone reporting.

10.1 Configuring the reporting

You can configure the reporting parameters and options:

- DLOADX program: "VERSA – Reporting" window.
- functions available in the MONITORING submenu (SERVICE MODE ▶5. MONITORING).

All parameters and options of reporting can only be configured by means of the DLOADX program.

10.2 Reporting parameters and options

REPORTING – TELEPHONE and REPORTING – ETHM options are described in the "Global options" section (p. 27).

10.2.1 Options

Station 1 or 2 – select this option if the control panel is to send event codes to Station 1, and in the case of failure – to Station 2.

Station 1 – select this option if the control panel is to send event codes to Station 1 only.

Station 2 – select this option if the control panel is to send event codes to Station 2 only.

Station 1 and 2 – select this option if the control panel is to send event codes to both monitoring stations.

Events amount limiting – if the option is enabled, events from the same source are saved into the event log and reported to the monitoring station 3 times only. This option does not apply to the alarms from zones (see: AUTO-RESET 3 or AUTO-RESET 1 zone option).

Report module restarts – if the option is enabled, in case of sending event codes in Contact ID or SIA format, the monitoring station is informed about module restarts.

Restore after bell – if the option is enabled, the zone restore code will only be sent to the monitoring station after the alarm signaling ends. If a few outputs are signaling alarm, the zone restore code will be sent when one of them stops signaling the alarm.

Restore after disarm – if the option is enabled, the zone restore code will only be sent to the monitoring station after disarming the partition to which the zone belongs.

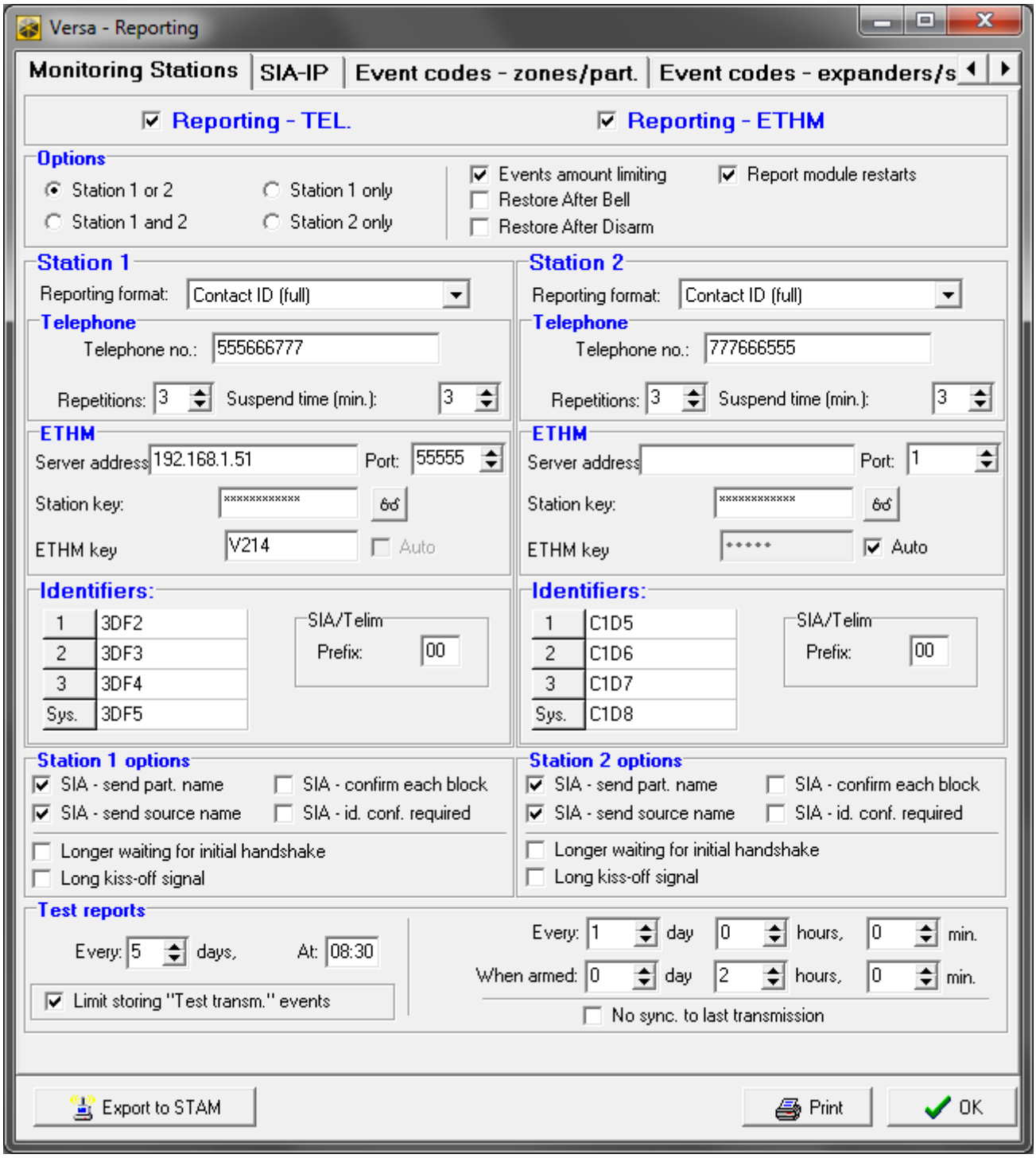


Fig. 21. DLOADX program: “Monitoring Stations” tab in “VERSA – Reporting” window.

10.2.2 Station 1 / Station 2

Reporting format – format in which event codes are sent to the monitoring station.

In the TELIM format, events can only be sent via the analog telephone line.

Telephone

Telephone no. – telephone number of the monitoring station.

Repetitions – the number of attempts to send an event code via the telephone line. If all attempts fail, the control panel will suspend reporting via the telephone line. Up to 31 retries can be programmed. Programming the value 0 means that monitoring will be suspended after 8 attempts.

Suspend time – the time for which reporting will be suspended, if attempts fail to send an event code through all provided transmission paths. The control panel will resume the attempt of establishing telephone connection with the monitoring station after this time expires or a next, new event occurs. Up to 30 minutes can be programmed. Programming the value 0 means that an attempt to establish telephone connection with the monitoring station will only be taken after occurrence of a new event in the system.

ETHM

Server address – network address of the monitoring station for reporting via Ethernet or. You can enter either the IP address or the domain name.

Port – number of port used for communication between the control panel and the monitoring station. You can enter a value from 1 to 65535.

Station key – a string of up to 12 alphanumeric characters (digits, letters and special characters), which is used for encryption of data sent to the monitoring station.

ETHM key – a string of up to 5 alphanumeric characters to be used for identification of the control panel for the purposes of reporting via Ethernet.

Identifiers

Event codes are sent to the monitoring station with one of the four identifiers:

- identifier 1 – events from zones (alarms, tampers, troubles),
- identifier 2 – alarms triggered from keypad, arming/disarming by means of zones, quick arming, loss of communication with wireless devices, as well as expander troubles and tampers,
- identifier 3 – arming/disarming and alarm clearing by means of code or proximity card,
- system identifier – power supply troubles, zone bypasses, troubles of control panel high-current outputs, communication bus trouble, programming related events, etc.

The identifier consists of 4 hexadecimal characters (digits or letters from A to F). Entering the value 0000 means that events assigned to that identifier will not be reported. Using the digit 0 in the identifiers is not recommended.

SIA / TELIM prefix – 2 characters which will precede each of the identifiers in case of the SIA and TELIM formats. Thus an identifier consisting of 6 characters can be obtained. 2 hexadecimal characters (digits or letters from A to F) can be programmed. Entering 00 means that the prefix will not be added. Using the digit 0 in the prefix is not recommended.

Station 1 options / Station 2 options

SIA – send part. name – if the option is enabled, in the SIA format, the name of partition where the event took place will also be sent, in addition to the event code.

SIA – send source name – if the option is enabled, in the SIA format, the name of event source (zone, user, etc.) will also be sent, in addition to the event code.

SIA – confirm each block – if the option is enabled, the control panel will wait for acknowledgement by the monitoring station of receiving every data block sent in the SIA format. The option applies to telephone reporting.

SIA – id. conf. required – if the option is enabled, the control panel will wait for acknowledgement by the monitoring station of receiving the identifier with which the data were sent. The option applies to telephone reporting.

Longer waiting for initial handshake – if the option is enabled, the control panel will wait longer for handshake from the monitoring station in case of sending events in the Ademco Express, Contact ID or SIA format. Enable this option in the event of telephone reporting, if the monitoring station sends a non-standard initial handshake.

Long kiss-off signal – if the option is enabled, the control panel will accept a long kiss-off (acknowledgment) signal for receiving events in case of Ademco Express and Contact ID formats. Enable this option in the event of telephone reporting, if the monitoring station acknowledges receiving events in a non-standard way (the kiss-off signal is longer than 800 ms).

10.2.3 Test transmissions

The test transmission may be sent:

- at a specified time. The test transmission code will be sent regularly at a defined time. The number of days between transmissions and the time of sending transmission are programmed. Programming the value 0 for days means that the transmission will be sent everyday (in the same way, as in case programming the value 1).
- in specified time intervals. You can program the time intervals in which test transmissions are to be sent when the system is disarmed and when the system is armed (number of days, hours and minutes). The test transmission code will be sent:
  – after a predefined period of time has elapsed since the last transmission, irrespective of whether it was a test transmission, or the code of another event was sent (the NO SYNC. TO LAST TRANSMISSION option disabled),
  – at predefined time intervals (the NO SYNC. TO LAST TRANSMISSION option enabled).

10.3 SIA-IP

10.3.1 Monitoring station 1 / Monitoring station 2

IP format – if the event codes are to be sent via Ethernet, specify whether SATEL format or SIA-IP format (SIA DC-09 standard) will be used.

Protocol – if the event codes are to be sent via Ethernet, specify whether TCP or UDP protocol will be used.

Options – options related to SIA-IP format:

Send MAC address – if this option is enabled, the MAC address is sent with event code.

Send timestamp – if this option is enabled, the date and time are sent with event code (the monitoring station can change the date and time in the control panel).

Encrypt data – if the option is enabled, the data being sent are encrypted, and the date and time are sent with event code (the monitoring station can change the date and time in the control panel).

SIA-IP key – the key to encrypt data to be sent using the SIA-IP format.

hex – if the option is enabled, you can enter up to 32 hexadecimal characters as the SIA-IP KEY. If the option is disabled, you can enter up to 16 alphanumeric characters as the SIA-IP KEY.

SIA-IP acct – a string of up to 16 hexadecimal characters, which is used to identify the control panel for the purpose of reporting in SIA-IP format.

Supervision interval – in the case of reporting in the SIA-IP format, an additional transmission can be sent at specified intervals to check communication with the monitoring

station. You can program a number of days, hours, minutes and seconds between the transmissions. Entering zeros only means that no additional transmission will be sent.

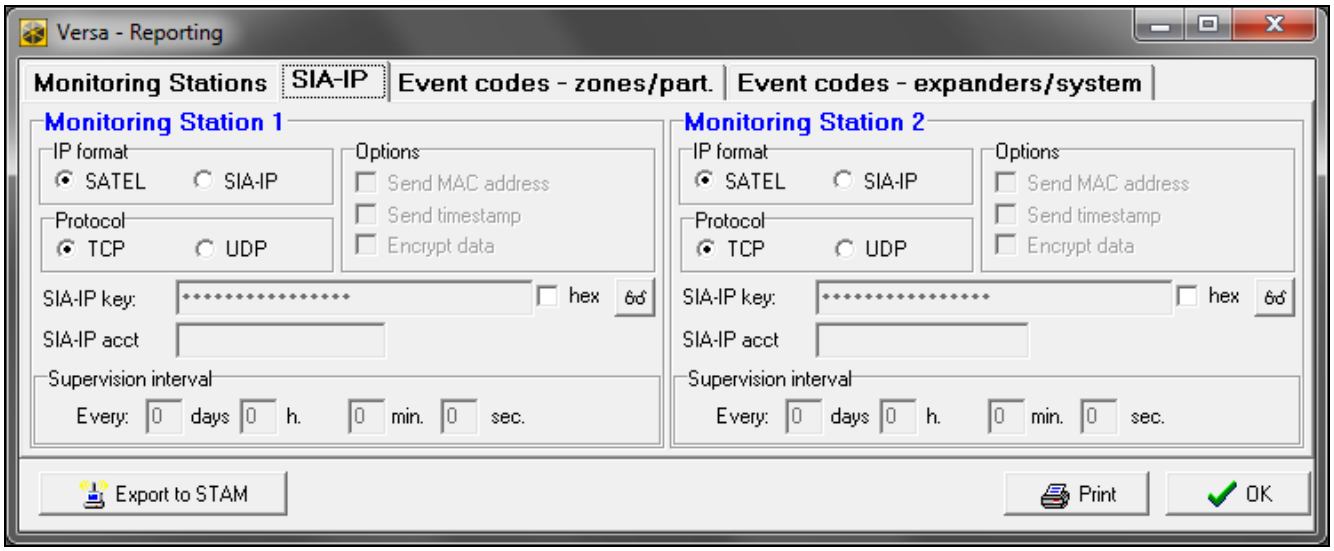


Fig. 22. DLOADX program: “SIA-IP” tab in “VERSA – Reporting” window.

10.4 Event codes

For the pulse and Ademco Express formats, it is necessary to program codes which will be reported to the monitoring station if the defined events occur. An event code consists of 2 hexadecimal characters (digits or letters from A to F). The reported events are those for which a code different from “00” has been programmed.

For the Contact ID and SIA formats, event codes consistent with format specification are sent. In case of the CONTACT ID (SELECTED) and SIA (SELECTED), the codes must be programmed at the events which are to be reported (not the programmed code, but a code consistent with the format specification will be sent).

10.5 Starting the reporting

1. Get the data necessary to properly start the reporting from the monitoring station operator:
   - depending on the transmission path:
     - telephone number of the monitoring station (reporting via telephone line),
     - server address, TCP port number, STATION KEY and ETHM KEY (reporting via Ethernet network).
   - transmission format required by the monitoring station,
   - identifiers assigned to the alarm system,
   - list of event codes (not applicable to Contact ID and SIA formats).
2. Determine whether the event codes will be sent to both monitoring stations or to one of them only (enable one of the options: STATION 1 OR 2, STATION 1, STATION 2 or STATION 1 AND 2).
3. Determine whether the number of events from the same source is to be limited (EVENTS AMOUNT LIMITING option).
4. Determine when the restore code is to be sent (RESTORE AFTER BELL, RESTORE AFTER DISARM options).

5. For the monitoring station to which event codes are to be sent:
   - define the format in which event codes will be sent (REPORTING FORMAT parameter),
   - if you select Ademco Express, Contact ID or SIA format, configure the additional options (SIA – SEND PART. NAME, SIA – SEND SOURCE NAME, SIA – CONFIRM EACH BLOCK, SIA – ID. CONF. REQUIRED, LONGER WAITING FOR INITIAL HANDSHAKE, LONG KISS-OFF SIGNAL),
   - program the identifiers to be sent with the event codes,
   - for the SIA or TELIM format, if the identifier is to consist of 6 characters, program SIA / TELIM PREFIX.
6. Define the parameters of test transmissions.
7. If a transmission format other than CONTACT ID (FULL) or SIA (FULL) is selected, program the codes for events which are to be reported.

10.5.1 Reporting via telephone line

1. Enable the REPORTING – TELEPHONE option (see: “Global options” p. 27).
2. Program the monitoring station parameters:
   – phone number,
   – the number of attempts to connect to the station after which, if there is no connection, the control panel will suspend reporting,
   – time for which reporting will be suspended after the programmed number of attempts to establish connection with the station has been made.
3. Configure the global options for telephone communicator:
   – determine how the telephone numbers should be dialed (TONE DIALING; in case of the pulse dialing option – PULSE 1/1,5 (OFF 1/2)),
   – determine whether the control panel, prior to dialing the number, should check the telephone line for dialing signal (NO DIAL TONE TEST),
   – determine the reaction to signals received after dialing the number (NO ANSWER TONE TEST).

10.5.2 Reporting via Ethernet network

1. Enable the REPORTING – ETHM option (see: “Global options” p. 27).
2. Program the monitoring station parameters:
   – monitoring station address,
   – TCP port,
   – data encryption key (STATION KEY),
   – control panel identifier for the purposes of monitoring via Ethernet (ETHM KEY).
3. Define whether the events are to be sent in SATEL format or SIA-IP format (IP FORMAT).
4. If the SIA-IP format is to be used, configure the additional options and parameters (SEND MAC ADDRESS, SEND TIMESTAMP, ENCRYPT DATA, SIA-IP KEY, HEX, SIA-IP ACCT and SUPERVISION INTERVAL).
5. Specify whether TCP or UDP protocol is to be used.
6. Configure the Ethernet module network settings.

11. Messaging

The control panel can send notifications about system events by phone or by means of e-mail messages.

11.1 Telephone messaging

The control panel can notify about system events by phone using:

- voice messages – connection of INT-VG module or CA-64 SM expander is required,
- text messages – they can be sent as SMS messages (connection of SATEL's GSM module is required) or PAGER type messages.

11.1.1 Configuring the telephone messaging

You can configure the telephone messaging parameters and options:

- DLOADX program: "VERSA – Tel. messaging" window.
- functions available in the MESSAGING submenu (SERVICE MODE ▶6. MESSAGING).

11.1.2 Parameters and options of the telephone messaging

TELEPHONE MESSAGING option is described in "Global options" section (p. 27).

Round count – the number of attempts made by the control panel to notify the selected telephone number about the event. You can program from 1 to 7.

Retries no. for one round – the number of attempts made by the control panel to get through during one round. You can program from 1 to 7.

Description – individual name of the telephone number (up to 16 characters).

Telephone no. – the telephone number to which messaging is effected.

The users having the PROGRAMMING right may edit the telephone numbers to be notified by means of the TEL. NUMBERS user function ([code] ✱ 🔥 ▶6. SETTINGS ▶4. TEL. NUMBERS).

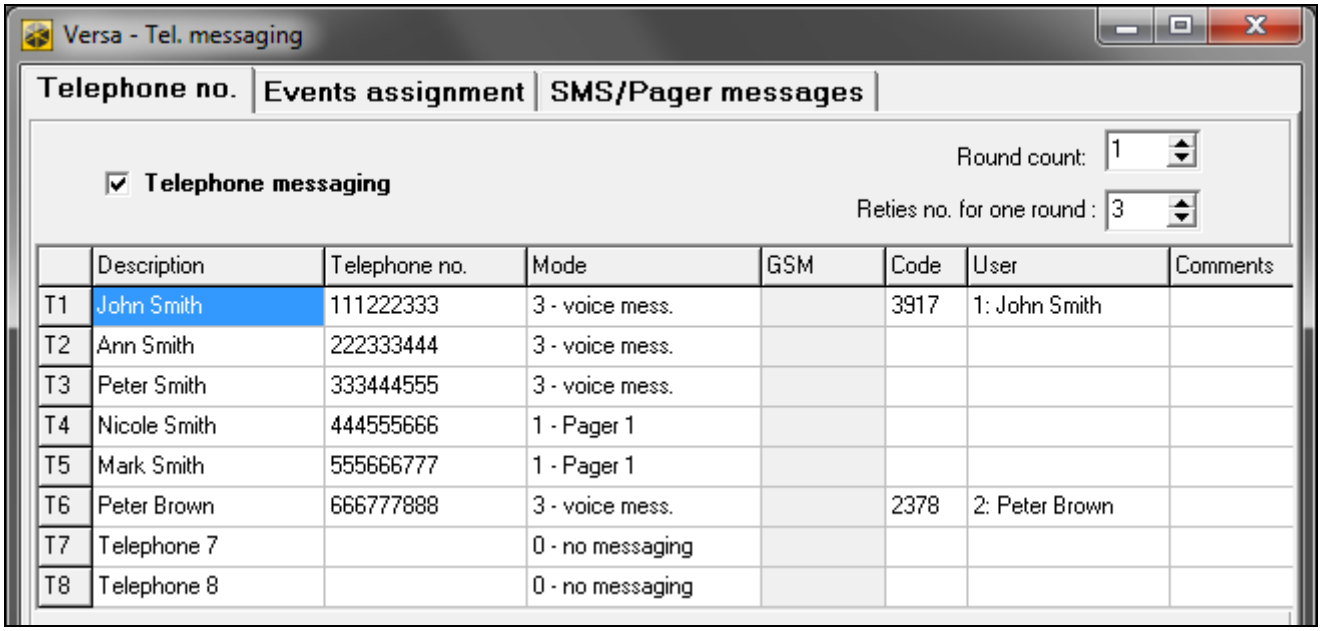


Fig. 23. DLOADX program: configuring the telephone messaging parameters.

Mode – selection of the form in which the indicated telephone number is to be notified (0 – no messaging, 1 – PAGER1, 2 – PAGER2, 3 – voice message, 4 – SMS).

Code – 4 digits which, if entered using the telephone keys, will acknowledge receipt of the voice notification and clear telephone messaging of the event.

By means of the MSG.CLR.CODES user function ([code] ✱ 🔥 ▶6. SETTINGS ▶5. MSG.CLR.CODES), the users having the PROGRAMMING right can edit the codes for acknowledging / clearing notification.

User – the user assigned to the phone number. If the user has the INT-VG ACCESS right and the INT-VG module is connected to control panel, he will get automatically access to the voice menu after acknowledging the voice notification.

11.1.3 Event assignment

Specify for the events, the occurrence of which is to be notified by the control panel:

- telephone numbers that will be notified,
- number of the message to be sent. You can assign the text message number to an event. In the case of voice notifications, the voice message assigned to that text message will be used.

11.1.4 SMS/Pager messages

You can program up to 64 text messages that will be used for notification. You can assign a voice message to each text message. The text messages are numbered from 1 to 64. The voice messages are numbered from 0 to 15 (INT-VG module / CA-64 SM expander can play back up to 16 voice messages). The same voice message can be assigned to several text messages.

For PAGER messaging, define the pager identification parameters.

11.1.5 Starting the telephone messaging

1. Enable the TELEPHONE MESSAGING option (see: “Global options” p. 27).
2. Define the number of attempts made by the control panel to notify about the event (parameters ROUND COUNT and RETRIES NO. FOR ONE ROUND).
3. Enter the phone numbers that are to be notified, and description of those phone numbers.
4. Specify, of which events, which phone numbers and by means of which messages the control panel is to notify (remember that a text message number is assigned to each event, and the voice message assigned to that text message will be used for voice notification).
5. Determine whether alarm clearing should cancel the messaging (global option CLEAR MESSAGING ON ALARM CLEARING).
6. Configure the global options related to telephone communicator:
   – determine how the telephone numbers should be dialed (TONE DIALING; in case of the pulse dialing option – PULSE 1/1,5 (OFF 1/2)),
   – determine whether the control panel, prior to dialing the number, should check the telephone line for dialing signal (NO DIAL TONE TEST),

PAGER / SMS messaging

1. Select PAGER1 or PAGER2 as the messaging type for the phone number to be notified.
2. Enter the content of messages that are to be used for notification.
3. Define the pager identification parameters (PAGER1 factory settings are configured for sending the message as SMS message via the SATEL GSM module).

Voice messaging

1. For the telephone number to be notified:
   – select voice messaging as the type of notification,

– enter the code, if the telephone user can confirm having listened to the voice message and clear the messaging,
– indicate the alarm system user, if the telephone user is to automatically get access to the voice menu after entering the code (the user must have the INT-VG ACCESS right).

2. Assign voice messages to text messages.
3. Record or synthesize the voice messages that are to be used for notification.
4. Determine whether the control panel is to play back the voice message after going off-hook, or 8/16 seconds after the dialing is completed (NO ANSWER TONE TEST).

11.2 E-mail messaging

E-mail messages are sent by means of the ETHM-1 Plus Ethernet module. The content of e-mail messages is automatically generated by the control panel.

11.2.1 Configuring the e-mail messaging

You can configure the parameters and options of e-mail messaging by means of the DLOADX program: "VERSA – Structure" window →"Hardware" tab →*[Ethernet module name]* →"Messaging" tab →"E-MAIL" tab. Before making any changes, click on the "Read" button, and after making the changes – on the "Write" button (the data relating to the e-mail messaging are not read after clicking on the  button or saved after clicking on the  button in the DLOADX program main menu).

11.2.2 Parameters and options of the e-mail messaging

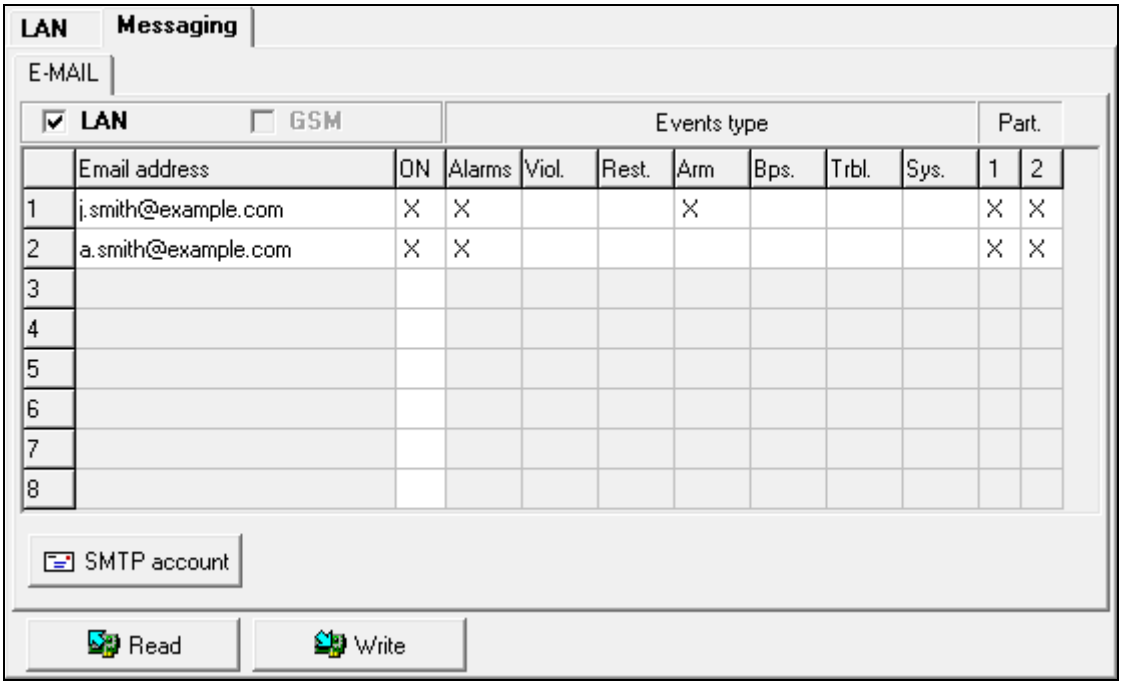


Fig. 24. DLOADX program: configuring the e-mail messaging.

LAN – if the option is enabled, the control panel can notify of occurrence of specified events by means of e-mail messages.

Email address – e-mail address to which messages are to be sent for notification of events.

Because the message is sent to many recipients, the addressees are hidden. If you want the addressee to be shown, place @ before the email address (e.g. @j.smith@example.com).

ON – with this option enabled, it will be possible to send messages to the given e-mail address for notification of events.

Events type – define of which events the given e-mail address is to be notified.

Part. – define the partitions, about the events from which the given e-mail address is to be notified.

SMTP account – click to open the “SMTP account” window.

Read – click to read data from the module.

Write – click to write data to the module.

SMTP account

It is required to have an e-mail account so as to enter its parameters in the DLOADX program for the purpose of e-mail messaging.

Mail server (SMTP) – address of outgoing mail server.

Server port – number of outgoing mail port.

User name – name of the e-mail account used for authorization by the SMTP server (login to e-mail account).

Password – the password used for authorization by the SMTP server.

Encryption – you can define if and how the outgoing mail is encrypted:

none – outgoing mail is not encrypted.

STARTTLS – outgoing mail will be encrypted using the STARTTLS protocol.

SSL/TLS – outgoing mail will be encrypted using the SSL/TLS protocol.

Subject – subject of the e-mail message. It will be inserted in each e-mail message to be sent.

Sender address – e-mail address which will be inserted in the outgoing e-mail message as the sender address. If this field is blank, the name of e-mail account will be treated as the sender address.

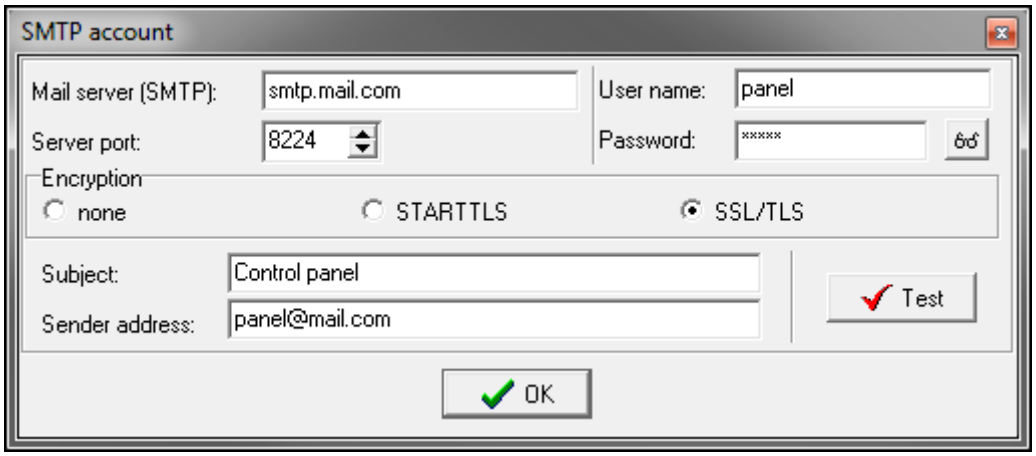


Fig. 25. DLOADX program: entering the data of e-mail account that will be used for e-mail messaging. The presented settings are just an example.

11.2.3 Starting the e-mail messaging

1. Enable the LAN option.
2. Enter the e-mail addresses to be notified, and enable the ON option for those addresses.
3. Define the events of which the control panel is to notify.

4. Configure the parameters of e-mail account which is to be used for sending e-mail messages (MAIL SERVER (SMTP), SERVER PORT, USER NAME, PASSWORD, ENCRYPTION, SENDER ADDRESS).
5. Enter the subject for e-mail messages.
6. Configure the Ethernet module network settings.

12. User schedules

The control panel offers 5 user schedules. The user schedule defines the user rights. When adding or editing a user, one of the user schedules is selected.

The default settings of keyfob are tied to the user schedule. If a keyfob is assigned to the user, the default keyfob settings will be suitable for the user schedule.

Changing the rights in user schedule results in a change of rights of all the users to whom that schedule was assigned.

Changing the keyfob default settings has no effect on the settings of keyfobs which are already added to the users.

12.1 Configuring the user schedules

You can configure the user schedules:

- DLOADX program: "VERSA – Users" window →"Users Schedules" tab (Fig. 26).
- functions available in the USR TEMPLATES submenu (SERVICE MODE ▶8. USR TEMPLATES).

12.2 Parameters of the user schedule

Schedule name – individual name of the user schedule (up to 16 characters).

Right – defines which functions are available to the user. The following rights are available:

Arming – the user can arm the system.

Disarming – the user can disarm the system.

Alarm clearing – the user can clear alarms.

Tel. mess. clearing – the user can cancel messaging by means of the ABORT V.MSG. user function (if he has at same time the ALARM CLEARING right and the CLEAR MESSAGING ON ALARM CLEARING global option is enabled, the messaging will be automatically canceled when the alarm is cleared).

Auto-arming defer – using the A-ARM DEFER. function ([CODE] [*] ▶6. SETTINGS ▶1. A-ARM DEFER.), the user can defer arming by the timer.

Zone inhibition – the user can inhibit the system zones by means of the INHIBIT function ([CODE] [*] ▶4. BYPASSES ▶1. INHIBIT).

Zone isolation – using the ISOLATE function ([CODE] [*] ▶4. BYPASSES ▶1. ISOLATE), the user having additionally the ZONE INHIBITION right can isolate the system zones.

Change access code – the user can change own access code (CHANGE CODE function).

Users editing – the user can add, edit and delete users (USERS function).

Control – the user can control the outputs by means of the CONTROL function.

Programming – the user has access to the SETTINGS function, which allows him to program the control panel clock, timers, telephone numbers for messaging and codes to clear messaging.

DOWNLOAD/SERVICE – the user can define the rules of service access, initiate remote programming of the control panel from the keypad and replace batteries in the wireless keypads.

Inspection – the user has access to the EVENT LOG and SYSTEM STATE functions. In case of arming by means of the LCD keypad, the user gets information about bypassed zones and causes of denial of arming, if any (the user can enforce the arming).

Tests – the user has access to the TESTS submenu.

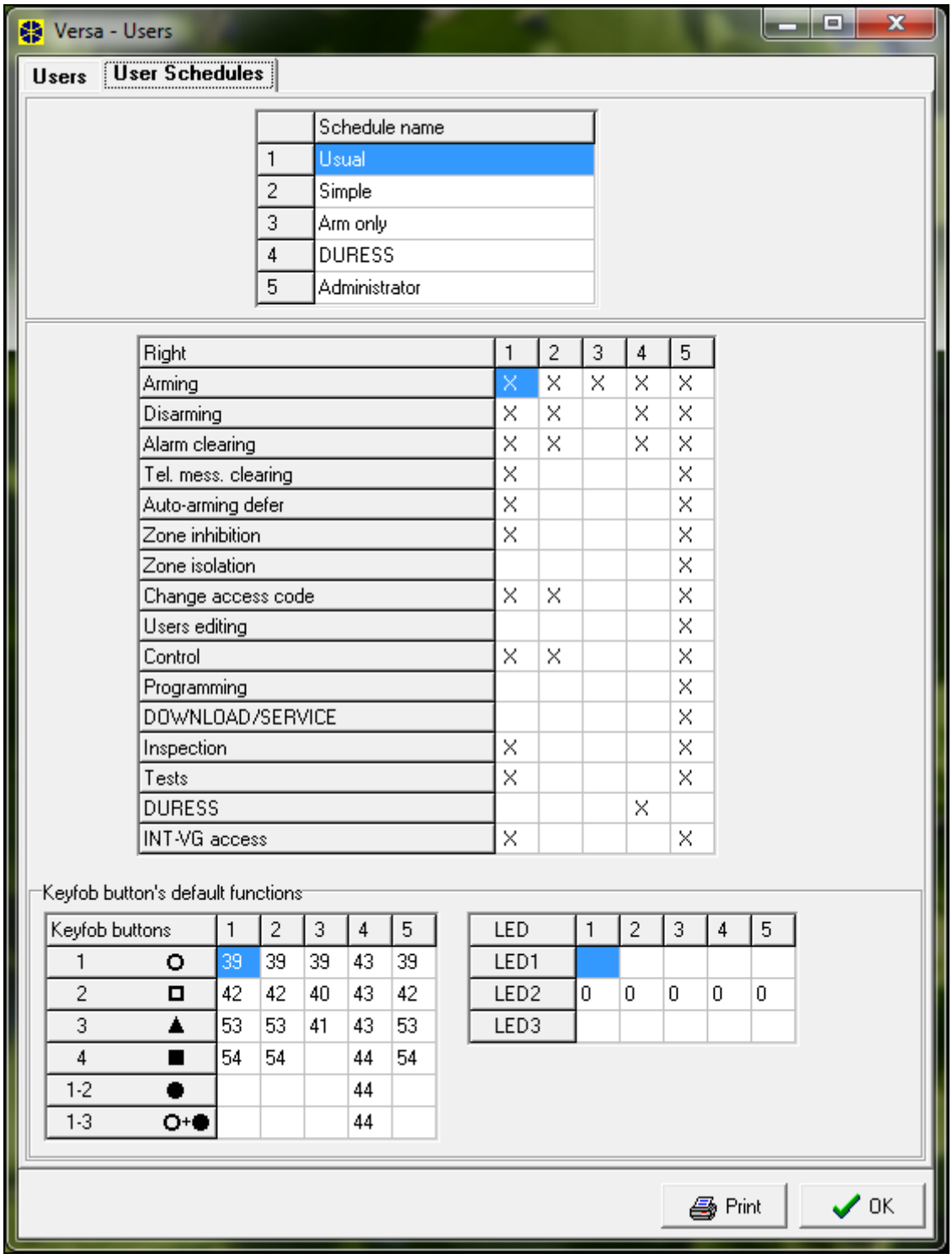


Fig. 26. DLOADX program: “User Schedules” tab in “VERSA – Users” window.

DURESS – a special right that allows to define in the system a code/card which, if used for arming/disarming or alarm clearing, will trigger a silent alarm (which is signaled in no

way, but the alarm code is sent to the monitoring station). The alarm will be triggered in the partition in which alarm would be triggered in the event of tamper of the keypad/proximity card arm/disarm device used for arming/disarming or alarm clearing.

INT-VG access – the user can operate the control panel by means of a telephone (DTMF), using the interactive voice menu.

12.3 Functions assigned to keyfob buttons

Functions that can be assigned to the keyfob buttons are numbered, which makes easier their programming in the keypad (you can also scroll through the list using the ✕▼ and ⚿▲ keys).

In the LED keypad, the function number is presented in binary form on the LEDs 1-12, in the same way as the decimal values (see: page 10 Table 4). Only values corresponding to the function numbers can be entered.

0. Not used

1. Zone 1 violation
2. Zone 2 violation
3. Zone 3 violation
4. Zone 4 violation
5. Zone 5 violation
6. Zone 6 violation
7. Zone 7 violation
8. Zone 8 violation
9. Zone 9 violation
10. Zone 10 violation
11. Zone 11 violation
12. Zone 12 violation
13. Zone 13 violation
14. Zone 14 violation
15. Zone 15 violation
16. Zone 16 violation
17. Zone 17 violation
18. Zone 18 violation
19. Zone 19 violation
20. Zone 20 violation
21. Zone 21 violation
22. Zone 22 violation
23. Zone 23 violation
24. Zone 24 violation
25. Zone 25 violation
26. Zone 26 violation
27. Zone 27 violation
28. Zone 28 violation
29. Zone 29 violation
30. Zone 30 violation

31. Arming partition 1 – full armed mode
32. Arming partition 1 – night armed mode

33. Arming partition 1 – day armed mode
34. Disarming / clearing alarm in partition 1
35. Arming partition 2 – full armed mode
36. Arming partition 2 – night armed mode
37. Arming partition 2 – day armed mode
38. Disarming / clearing alarm in partition 2
39. Arming partitions 1 and 2 – full armed mode
40. Arming partitions 1 and 2 – night armed mode
41. Arming partitions 1 and 2 – day armed mode
42. Disarming / clearing alarm in partitions 1 and 2
43. Loud panic alarm
44. Silent panic alarm
45. Fire alarm
46. Medical alarm

51. Output 1 activation
52. Output 2 activation
53. Output 3 activation
54. Output 4 activation
55. Output 5 activation
56. Output 6 activation
57. Output 7 activation
58. Output 8 activation
59. Output 9 activation
60. Output 10 activation
61. Output 11 activation
62. Output 12 activation

71. Output 1 deactivation
72. Output 2 deactivation
73. Output 3 deactivation
74. Output 4 deactivation
75. Output 5 deactivation
76. Output 6 deactivation
77. Output 7 deactivation
78. Output 8 deactivation
79. Output 9 deactivation
80. Output 10 deactivation
81. Output 11 deactivation
82. Output 12 deactivation

91. Output 1 switchover
92. Output 2 switchover
93. Output 3 switchover
94. Output 4 switchover
95. Output 5 switchover
96. Output 6 switchover
97. Output 7 switchover
98. Output 8 switchover
99. Output 9 switchover

100. Output 10 switchover
101. Output 11 switchover
102. Output 12 switchover

12.4 Confirmation on LEDs in the APT-200 / APT-100 keyfob

The list of information that may be presented on the keyfob LEDs is numbered, which makes programming easier (use the ✕▼ and 🔑▲ keys to scroll through the list in the keypad). In the LED keypad, the number is presented in binary format on LEDs 1-12, in a similar way as the decimal values (see: page 10, Table 4). Only the values corresponding to the numbers on the list can be entered.

0. On	*LED is ON when the control panel has confirmed receiving information on a keypress*
1. Output 1 state	*LED is ON when the selected output is active*
2. Output 2 state	
3. Output 3 state	
4. Output 4 state	
5. Output 5 state	
6. Output 6 state	
7. Output 7 state	
8. Output 8 state	
9. Output 9 state	
10. Output 10 state	
11. Output 11 state	
12. Output 12 state	
13. Arming: Partition 1	*LED is ON when partition 1 is armed*
14. Arming: Partition 2	*LED is ON when partition 2 is armed*
15. Arming: Partition 1 or 2	*LED is ON when partition 1 or 2 is armed*
16. Arming: Partition 1 and 2	*LED is ON when partitions 1 and 2 are armed*
17. Partition 1 – Full arm	*LED is ON when partition 1 is fully armed*
18. Partition 1 – Night arm	*LED is ON when partition 1 is armed in night mode*
19. Partition 1 – Day arm	*LED is ON when partition 1 is armed in day mode*
20. Partition 2 – Full arm	*LED is ON when partition 2 is fully armed*
21. Partition 2 – Night arm	*LED is ON when partition 2 is armed in night mode*
22. Partition 2 – Day arm	*LED is ON when partition 2 is armed in day mode*
23. Partition 1 – Alarm	*LED is ON when there is alarm in partition 1*
24. Partition 2 – Alarm	*LED is ON when there is alarm in partition 2*
25. Partition 1 or 2 – Alarm	*LED is ON when there is alarm in partition 1 or 2*
26. Trouble	*LED is ON when there is trouble in the system*
27. Partition 1 – Not armed	*LED is ON when partition 1 is disarmed*
28. Partition 2 – Not armed	*LED is ON when partition 2 is disarmed*
29. Partition 1+2 – Not armed	*LED is ON when partitions 1 and 2 are disarmed*
255. NOT PRESENT	*LED will not be used for confirmation*

13. Compliance with EN 50131 standard requirements for Grade 2

To meet the requirements of EN 50131 standard for Grade 2, do the following:

- enable the global options:
  - GRADE 2,
  - TROUBLE MEMORY UNTIL REVIEW,
  - EVENTS AMOUNT LIMITING (in the DLOADX program, the option is available in the reporting options),
  - BLOCK AFTER 3 UNKNOWN CODES/CARDS.
- disable the global options:
  - TAMPER ALARM ALWAYS AUDIBLE,
  - ARM EVEN IF NOT READY AFTER EXIT DELAY.
- program the AC loss time after which a trouble will be reported to be no longer than 60 minutes (AC LOSS REPORT DELAY global parameter),
- in case of arming by means of timers, program the suitable auto-arming delay in partitions so that the system users can be warned of the automatic arming,
- program the entry delay to be no longer than 45 seconds,
- enable the AUTO-RESET 3 option for all burglary zones,
- disable the ALARM ON EXIT DELAY END option for alarm zones beyond the exit route,
- enable the BYPASS DISABLED option for tamper, panic and trouble zones,
- remember that the operation time of acoustic sirens should be minimum 90 seconds and maximum 15 minutes (which requires suitable configuration of the cut-off time of alarm signaling outputs).

14. Control panel firmware update

1. Download the update program for control panel firmware from www.satel.eu.
2. Connect the control panel RS-232 (TTL) port with the computer port (for example, using the USB-RS converter offered by SATEL).
3. Update the control panel firmware, using one of the methods described below.

When the firmware update is running, the control panel does not execute its normal functions.

14.1 Standard update procedure

1. Use the keypad to enter the service mode (enter the service code and press [*], and then [0] [0] [#]).
2. Press in turn [0] [9wxyz] [#]. The STARTER function will start. The control panel will be waiting until communication with the firmware updating program is established (you can terminate the STARTER function by pressing [*]).
3. Run the update program for control panel firmware.
4. Click on the  button.
5. In the window that will be displayed, indicate the COM port of the computer to which the control panel is connected and click “OK”. The firmware updating program will establish communication with the control panel.

6. When a prompt window is displayed asking you whether to continue the firmware update, click “Yes”. The control panel firmware will be updated.

14.2 Emergency update procedure

If the control panel does not support keypads, does not accept the service code, etc., you can make use of the following procedure to update the control panel firmware.

1. Run the update program for control panel firmware.
2. Click on the  button.
3. In the window that will be displayed, indicate the COM port of the computer to which the control panel is connected, check the RESTART option and click “OK”.
4. Power off the control panel (disconnect AC mains first, and the battery next).
5. Power up the control panel (first connect the battery and then the AC power).
6. The firmware updating program will establish communication with the control panel.
7. When a prompt window is displayed asking you whether to continue the firmware update, click “Yes”. The control panel firmware will be updated.

The control panel will only wait 10 seconds after power-up for the firmware update to begin.

15. Manual update history

The table presents changes made since version 06/15.

Manual version	Introduced changes
10/15	• Information on the required DLOADX program version has been updated (p. 17). • Description of the SERVICE MESSAGE AFTER TAMPER ALARM option has been modified (p. 28). • Description of the SIGNALING ON INTERNAL SIRENS option has been added (p. 39). • Table indicating how the zone options are presented in keypads has been updated (p. 40). • Description of the 22. ETHM TROUBLE STATUS output function has been added (p. 42). • List of troubles, the occurrence of which can trigger the 22. ETHM TROUBLE STATUS function output has been added (p. 43). • Description of the PULSE output option has been modified (p. 45). • Table indicating how the output options are presented in keypads has been updated (p. 46). • Information on the VERSA-LCDR keypad has been added in the volume configuration section (p. 49).
04/16	• Information on required DLOADX program version has been updated (p. 17). • Description of ENTRY DELAY IN DAY ARM option has been added (p. 33). • Section “Proximity cards” has been added (p. 50). • Description of USER CAN REPLACE VERSA-LCDM-WRL BATTERY option has been added (p. 54). • Information on ASP-100 siren has been added (pp. 54, 57, 57, 59 & 62). • Information on AOD-200 detector has been added (pp. 56, 58 & 61). • Section “ABAX 2 / ABAX wireless sirens” has been modified (p. 64).
11/17	• Information on required DLOADX program version has been updated (p. 17). • Description of BACKLIGHT OFF ON AC LOSS option has been added (p. 29). • Description of ENTRY DELAY IN NIGHT ARM option has been added (p. 33).

	• Section “Hardware” has been added (p. 40). • Name of the SATEL SERVER (LAN) option has been changed to LAN (p. 51). • Description of DO NOT REPORT SATEL SERVER CONNECTION TROUBLE option has been added (p. 51). • Description of ALARM 3 INCORRECT CODES (MOBILE APPLICATION) option has been added (p. 52). • Description of PUSH NOTIFICATIONS option has been added (p. 52). • Information about QR code, that makes configuring mobile application easier, has been added (p. 52). • Name of the GET DATE AND TIME FROM A TIME SERVER (LAN) option has been changed to LAN (p. 53). • Description of USER CAN REPLACE VERSA-LCDM-WRL BATTERY option has been updated (p. 54). • Information on AOCD-250 detector has been added (p. 56, 58 and 60). • Information on ASD-150 detector has been added (p. 56, 59 and 62). • Information on reporting trouble by ACX-201 expander has been added (p. 65). • Name of the E-MAIL MESSAGING (LAN) option has been changed to LAN (p. 78). • Description of the DOWNLOAD/SERVICE right has been updated (p. 81). • Section “Confirmation on LEDs in the APT-200 / APT-100 keyfob” has been updated (p. 84).
09/21	• Information about ABAX 2 system devices has been added. • Information on required DLOADX program version has been updated (p. 17). • Description of AC LOSS REPORT DELAY parameter has been modified (p. 30). • Description of TEL. LINE LOSS REPORT DELAY parameter has been modified (p. 30). • Description of SILENT option has been modified (p. 49). • Section “ABAX 2 / ABAX wireless system controller” has been updated (p. 53). • Section “MICRA wireless system controller” has been updated (p. 66). • Section “Proximity card arm/disarm device” has been updated (p. 67). • A note on presenting e-mail addresses for e-mail messaging has been added (p. 78).